FASTHUB SOLUTIONS LIMITED
business@fasthub.co.tz
P.O.Box: 31206 Dar es salaam
Call: 0800 712 354 **"Toll Free"**
www.fasthub.co.tz

# Privacy Policy

FASTHUB SOLUTIONS LIMITED
business@fasthub.co.tz
P.O.Box: 31206 Dar es salaam
Call: 0800 712 354 "Toll Free"
www.fasthub.co.tz

# Process Management

| | |
|---|---|
| **Process Owner** | Data Protection Officer [DPO] |
| **Department** | Compliance |
| **Document Level** | Policy |
| **Document Effective Date** | 15 July 2025 |
| **Recommendation Level** | Risk Management Committee (RMC) & DPO |
| **Approval Level** | Board of Directors |

**Review History**

| Amendment | Reviewed By | Date | Approved by | Date | Version |
|---|---|---|---|---|---|
| Annual Review | (RMC) & DPO | | Board of Directors | | 1 |
| | | | | | |
| | | | | | |

Approved by:

Managing Director, FastHub Solutions

Signature: _____

# Table of Contents

1. Introduction.....3

2. Interpretation and Definitions.....3

3. What Personal Data Fasthub Processes.....4

4. How Fasthub Collects Personal Data.....4

5. Lawful Basis for Processing Personal Data.....5

6. Purpose of Data Processing.....6

7. Sharing of Personal Data.....6

9. Data Security Measures.....8

10. Your Rights as a Data Subject.....9

11. International Data Transfers.....9

12. Children's Data.....10

13. Changes to This Privacy Policy.....10

## 1. *Introduction*

About Fasthub

Fasthub is a licensed Tanzanian company that combines Financial Technology (FinTech) and Telecommunications Services. We're on a mission to make telecom and payment services easier for businesses. We do this by providing powerful solutions that work on both feature phones and smartphones. These solutions are designed to help modern organizations with digital transformation, financial inclusion, and real-time customer engagement.

Every solution we offer comes with customizable support, real-time analytics, and flexible integration options.

Our Commitment to Data Privacy

It's important to understand that Fasthub acts as a *data processor*. This means we don't decide why or how your personal data is processed. Instead, we process personal data on behalf of our clients, who are the data controllers. We strictly follow their instructions, our contracts, and the Tanzania Personal Data Protection Act, 2022. We are dedicated to maintaining the highest standards of data privacy, operational transparency, and information security across all our services.

## 2. *Interpretation and Definitions*

| | |
|---|---|
| **Personal Data** | Any information relating to an identified or identifiable natural person. This may include *names, contact details, identification numbers, transactional data, or online identifiers.* |
| **Sensitive Personal Data** | A special category of personal data that includes biometric data, health records, religious beliefs, political opinions, ethnic origin, or criminal records. Processing such data requires additional legal justification and safeguards. |
| **Data Subject** | An individual whose personal data is collected or processed. [*Data subjects are entitled to exercise rights over their personal data].* |
| **Data Controller** | The entity [individual, organization, or public body] that determines the purpose and manner of processing personal data. Fasthub's clients typically act as controllers. |
| **Data Processor** | The entity that processes personal data on behalf of a data controller. |
| **Processing** | Any operation performed on personal data including collection, recording, organization, storage, alteration, retrieval, use, dissemination, restriction, deletion, or destruction. |

| | |
|---|---|
| **Third Party** | Any external entity other than the data subject, controller, or processor authorized to access or process data under the controller's instructions. |

## *3. What Personal Data Fasthub Processes*

As a **data processor**, Fasthub handles personal data on behalf of our clients for specific, legal reasons that they determine. The types of personal data we might process depend on the services we're providing. This could include;

| | | |
|---|---|---|
| **Data Processed** | **Full name and contact details** | Such as phone numbers and email addresses. |
| | **National ID or passport number** | This is typically used for verification services |
| | **Mobile money transaction metadata** | Including details like amounts, unique reference codes, and timestamps of transactions. |
| | **SMS or USSD responses** | When applicable, we process responses from customer surveys or notifications sent via these channels. |
| | **IP address or device identifier** | These are captured as part of our security and logging protocols to ensure the integrity and safety of our services. |
| | **KYC's [Business registration or license details]** | This applies specifically to corporate services where such information is necessary on any new client we onboard *[Due Diligency]* |

## *4. How Fasthub Collects Personal Data*

At Fasthub, we collect and process personal data strictly according to the instructions of our clients, who are the data controllers. The ways we collect data depend on the specific service we're providing. Here are the common methods;

| | | |
|---|---|---|
| **Process** | **API Integration** | Personal data is often sent to us through secure Application Programming Interfaces (APIs) that connect to our systems. This happens for services like mobile money transactions, identity verification, and SMS communications. |
| | **USSD and SMS Interfaces** | For services such as surveys, alerts, or queries, we may collect information that users enter directly via USSD (Unstructured Supplementary Service Data) or SMS (Short Message Service) channels |
| | **Batch File Uploads** | Our clients might provide us with structured data files that contain personal data. We process these files for tasks like bulk transactions, disbursements, or marketing campaigns. |
| | **Real-time Transactional Logs** | When we operate payment platforms or digital gateways, we automatically receive metadata. This includes details like timestamps, reference IDs, and source channels related to transactions. |
| | **Call Center Interactions** | If we're hosting IVR (Interactive Voice Response) or customer support services for a client, we may record call logs, menu selections, or routing information precisely as directed by that client. |

## 5. *Lawful Basis for Processing Personal Data*

As a data processor, Fasthub does not independently determine the legal grounds for processing personal data.This crucial responsibility rests entirely with our clients, who are the data controllers. However, we commit to ensuring that all personal data processing activities adhere strictly to the following principles;

A. *Reliance on Written Instructions*: We act only on explicit, written instructions from the data controller. These instructions clearly specify the lawful purpose for processing personal data, as defined and required under Tanzanian law, particularly the Tanzania Personal Data Protection Act, 2022.

B. *Valid Data Processing Agreements (DPAs):* All personal data processing we undertake is covered under a valid Data Processing Agreement (DPA) or a comprehensive contractual agreement. These agreements meticulously define our obligations, responsibilities, and limitations regarding the handling of personal data, ensuring clarity and compliance for both parties.

C. *No Secondary or Unauthorized Use:* We guarantee that we do not use or share personal data for any secondary, unauthorized, or incompatible purposes beyond what is explicitly instructed by the data controller and outlined in our agreements. Your data remains secure and is used only for its intended purpose.

D. *Assistance with Compliance:* We actively assist our data controllers in fulfilling their obligations to demonstrate compliance with the Tanzania Personal Data Protection Act, 2022. This includes providing necessary information and support to help them meet their legal requirements concerning data protection.

## 6. *Purpose of Data Processing*

Fasthub processes personal data exclusively to deliver or support services specifically defined and requested by the data controller. The primary purposes for which we process data may include, but are not limited to, the following;

A. *Transaction Processing:* This involves processing personal data to initiate, confirm, or complete payments, transfers, or withdrawals through various mobile money services. This ensures that financial transactions are accurately and securely executed as per client instructions.

B. *Customer Communication:* We process data to enable the sending of personalized notifications, alerts, reminders, surveys, or acknowledgments to end-users on behalf of our clients. This facilitates effective and timely communication between our clients and their customers.

C. *Identity and Service Verification:* Personal data is processed to validate a customer's identity or subscription status prior to the delivery of a service. This helps in preventing fraud and ensuring that services are provided to authorized individuals.

D. *Reporting and Analytics:* We process data to generate comprehensive performance metrics, user interaction reports, and campaign outcomes for our clients. This allows businesses to gain valuable insights into their operations and customer engagement.

E. *Dispute Resolution:* In instances of service issues, we process relevant personal data to investigate and address failed transactions, duplicate messages, or escalated user complaints. This enables us to provide effective support and resolve discrepancies efficiently

## 7. *Sharing of Personal Data*

Fasthub understands the importance of keeping personal data private. We only share personal data with third parties when explicitly authorized by the data controller (our client) and always under strict contractual or regulatory controls. This ensures your data remains protected. Here are common scenarios where data might be shared;

A. Mobile Network Operators (MNOs), to services such as SMS delivery, USSD interactions, or mobile money transfers possible, certain data needs to be exchanged with the relevant telecom operators. This is essential for the functionality of these core services.

B. Technical Sub-processors, as we sometimes engage approved technology partners (such as providers for server hosting, cloud services, or encryption services) to deliver the necessary infrastructure for our services. When we do, we ensure these

sub-processors are contractually bound to uphold equivalent data protection, confidentiality, and security standards as Fasthub. They are not permitted to use the data for their own purposes.

C. Regulatory and Law Enforcement Bodies in very specific circumstances, and only when mandated under Tanzanian law, we may be required to disclose certain data to authorized government institutions. In such cases, we strive to inform the data controller of the request unless legally prohibited from doing so.

D. Affiliated Entities that data may be accessed by other companies within Fasthub under shared service agreements and always within applicable compliance boundaries and data protection regulations. This allows for efficient internal operations while maintaining data security.

To emphasize we ensure all recipients of personal data are contractually obligated to uphold the highest standards of confidentiality, security, and data protection, mirroring our own commitments under the Tanzania Personal Data Protection Act, 2022.

## 8. *Data Retention*

Fasthub is committed to responsible data handling, which includes not retaining personal data for longer than necessary. We retain personal data only for as long as needed to fulfill the purpose outlined by the data controller or to comply with specific legal or regulatory obligations [ BOT, TCRA & PDPC]. Our data retention approach is guided by the following principles;

A. Contractual Retention, the precise duration for which personal data is retained, is defined and agreed upon in the data processing agreement (DPA) or through explicit instructions provided by our clients. This ensures alignment with their specific business needs and compliance requirements.

B. Legal Obligations that we strictly adhere to sector-specific legal and regulatory requirements that mandate certain retention periods for data. For example, telecommunication or financial regulations in Tanzania often require that transaction records and related personal data be kept for a period typically ranging from 5 , 7 to 10years.

C. System Logs for operational integrity and security auditing, internal system logs are retained on a rolling basis. These logs contain metadata crucial for troubleshooting, security incident response, and compliance checks. However, they are securely purged once they exceed their operational usefulness and the defined retention period.

D. Secure Disposal at the end of the defined retention period, all personal data is subjected to secure deletion or anonymization.

## 9. *Data Security Measures*

At Fasthub, we take the protection of personal data incredibly seriously. We implement a comprehensive suite of robust security measures designed to safeguard data from

unauthorized access, alteration, disclosure, or destruction. Our multi-layered security protocols include;

A. We employ strong, industry-standard encryption for personal data both in transit (when it's being sent across networks) and at rest (when it's stored on our servers). This prevents unauthorised interception or exposure, meaning even if data were accessed, it would be unreadable without the proper decryption keys.
B. We maintain strict access control mechanisms to ensure that only authorized personnel with clearly defined roles and responsibilities can access personal data. Access is rigorously governed by role-based permissions (RBAC), ensuring that staff can only access the data absolutely necessary for their job functions. Furthermore, multi-factor authentication (MFA) is in place for access to sensitive systems, adding an extra layer of security beyond just passwords.
C. Our hosting facilities and data centers are protected by cutting-edge physical security measures. These include biometric access controls, comprehensive surveillance systems, and fire detection and suppression systems to protect against physical threats.
D. We utilize state-of-the-art firewalls and intrusion detection/prevention systems (IDS/IPS) to monitor and control network traffic, blocking suspicious activity. We also conduct regular vulnerability scans and penetration testing to proactively identify and address potential weaknesses, preventing cyber threats and network exploitation.
E. Our most critical security asset is our people. All Fasthub personnel who handle personal data undergo mandatory, regular data privacy and cybersecurity training. This ensures they are fully aware of their responsibilities, best practices, and the latest threats, fostering a culture of security.
F. We have a well-defined and regularly tested incident management plan in place. This plan outlines precise steps to effectively detect, report, contain, and remediate data breaches or security events promptly and efficiently, adhering strictly to regulated timelines and notification requirements under Tanzanian law.

## *10. Your Rights as a Data Subject*

Under the **Tanzania Personal Data Protection Act, 2022**, individuals whose personal data is being processed (referred to as **Data Subjects**) are granted several significant rights. It's important to note that the **Data Controller (our clients)** is responsible for facilitating these rights. As a data processor, Fasthub is fully committed to **cooperating with our controllers** to ensure these rights are honored;

A. Our client [data subjects] have the fundamental right to request clear and comprehensive information regarding the nature, scope, and purpose of their personal data being processed. This includes details about what data is held, why it's processed, and with whom it might be shared.

B. If the personal data is inaccurate or incomplete, Data Subjects have the right to request its correction or update. We will support our clients/Data Subjects in making these necessary adjustments promptly.
C. Right to Erasure (Right to be Forgotten) in other words Data Subjects may/can request the deletion of their personal data under certain lawful grounds, for example, if the data is no longer necessary for the purpose for which it was collected, or if you withdraw consent and there is no other legal basis for processing.
D. Data Subjects may request that the processing of their data be limited or temporarily suspended, for instance, when contesting its accuracy or the lawfulness of its processing. This means the data can be stored but not further processed.
E. Data Subjects have the right to object to the use of their personal data for certain specific purposes, such as direct marketing. Upon receiving a valid objection, the processing for that purpose must cease.This right allows Data Subjects to receive their personal data in a structured, commonly used, and machine-readable format.
F. Data Subjects can request data be transmitted directly to another data controller where technically feasible.

## *11. International Data Transfers*

In some specific cases, Fasthub may need to process or store personal data outside of Tanzania. When this occurs, international data transfers are handled with the utmost care and in strict compliance with legal and contractual safeguards to ensure data protection is maintained at the highest level. These safeguards include;

A. Any cross-border transfers of personal data are only performed with the explicit, documented approval and instruction of the data controller. Fasthub will not transfer data internationally without their clear direction.
B. Fasthub prioritize transferring data to countries that have been deemed by relevant authorities to possess adequate data protection standards comparable to those in Tanzania. If a transfer to a country without such a designation is necessary, Fasthub ensures it is conducted under robust contractual clauses that provide appropriate safeguards, such as Standard Contractual Clauses (SCCs) approved by relevant data protection authorities.
C. All international sub-processors and infrastructure partners involved in data transfers are rigorously vetted to ensure they meet Fasthub's stringent security and data protection requirements. They are then contractually obligated to maintain industry-standard data protection and cybersecurity practices that mirror our own commitments.
D. Fasthub reserves the right to audit any cross-border data handling mechanisms, processes, and partners as part of our ongoing commitment to compliance with regulatory expectations and our contractual obligations. This ensures continuous oversight of data protection standards.

## *12. Children's Data*

Fasthub is committed to protecting the privacy of children. We do not knowingly process personal data of children under the age of 18 without lawful authority or verifiable consent from a parent, legal guardian, or other legally recognized representative.

Clients who intend to offer services to children and consequently process their personal data are expressly required to implement all necessary compliance procedures as stipulated by the Tanzania Personal Data Protection Act, 2022. This includes, but is not limited to, robust age verification mechanisms, obtaining verifiable parental consent, and conducting thorough risk assessments specific to the processing of children's data.

Should Fasthub discover that personal data of a child has been processed without proper legal justification or the necessary authorization, we will promptly notify the relevant data controller. We will then take immediate remedial action, which includes the secure deletion of the data where required by law or client instruction.

## *13. Changes to This Privacy Policy*

Fasthub is committed to transparency and adapting to evolving legal and technological landscapes. Therefore, we **reserve the right to modify this Privacy Policy periodically** in response to new legal requirements, regulatory changes, operational developments, or advancements in technology. Any updates or revisions to this policy will be posted promptly on our official website to ensure accessibility. Furthermore, where applicable and depending on the significance of the changes, we will share updates directly with our clients through formal communication channels, such as email notifications or client portals.

For material changes that significantly affect the rights of data subjects or alter the scope of our data processing activities, we will ensure these are communicated in advance. This will allow sufficient time for our clients to review the updated terms and, if necessary, to engage in renegotiation of contractual agreements to reflect the new policy.

The 'Last Updated' date prominently displayed at the top of this Privacy Policy indicates the most recent version in effect, allowing you to easily identify when the policy was last revised.