

Module 1: Data Processing Activities of Hosting Providers.

Learning Outcomes:

- Understand how the Kenya Data Protection Act applies to Truehost's data processing activities.
- Identify data processing workflows specific to Truehost's services.
- Learn compliance requirements for Truehost as a data controller and processor.

Overview of Data Processing at Truehost

1. What is Data Processing?

Data processing refers to any operation or set of operations performed on personal data, whether manually or automatically.

Also, it can refer to any operation performed on personal data whether or not by automated means such as:

Collection, recording, organization, structuring

Storage, adaptation, alteration

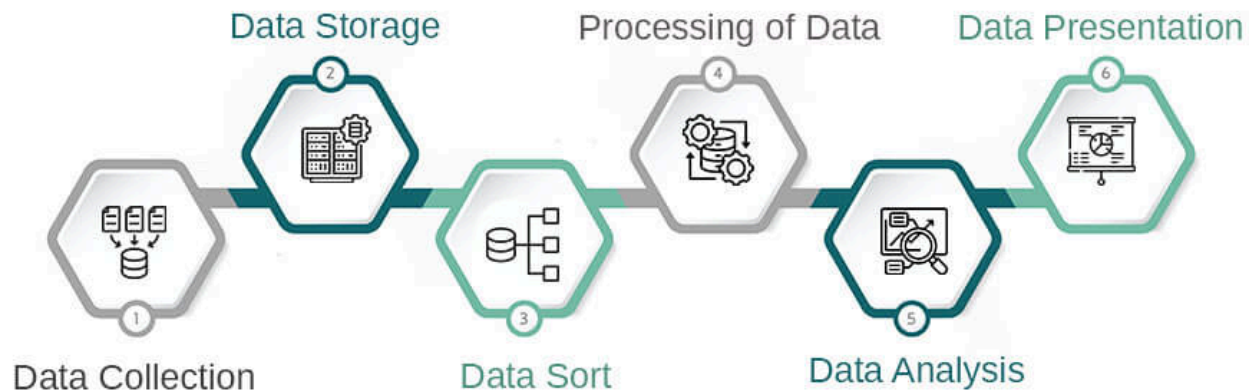
Retrieval, consultation or use

Disclosure (transmission, dissemination etc.)

Alignment, combination, restriction

Erasure and destruction

Data Processing

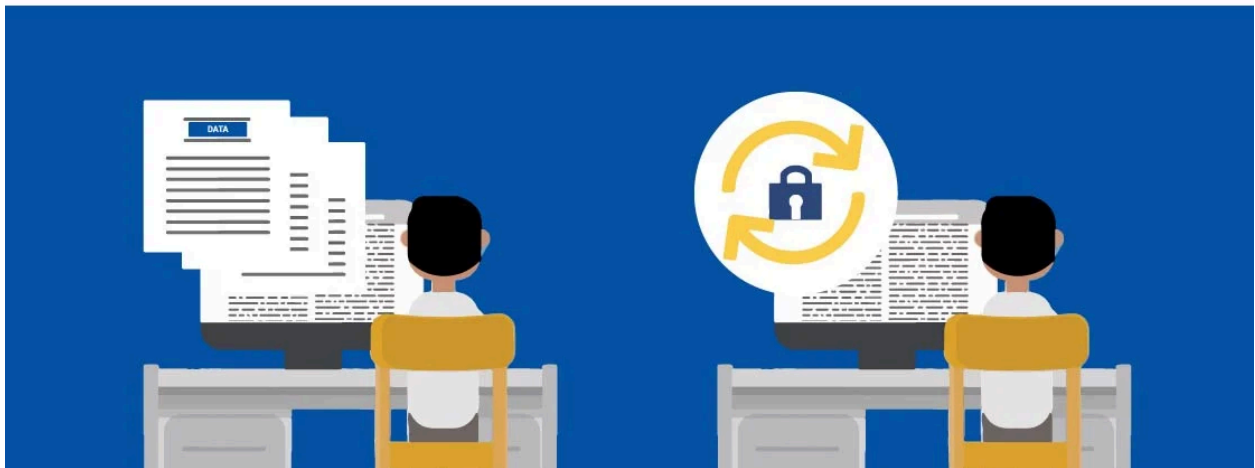


2. Who is a Data Processor?

Under the Kenya Data Protection Act, a **data processor** is any person or entity that processes personal data on behalf of a data controller (the entity that determines the purposes and means of processing). For Truehost:

- Truehost is a **data processor** when acting on behalf of clients (e.g., hosting websites or processing domain registration data).
- Truehost is also a **data controller** when collecting and processing data directly from customers (e.g., during account registration).

The Data Controller vs. Data Processor



3. What Kind of Data Does Truehost Process?

a. Personal Data:

This includes any information that identifies or can identify an individual. Examples:

- **Customer Account Information:** Names, email addresses, phone numbers, and billing details collected during service sign-up.
- **WHOIS Data:** Publicly accessible registration data for domains unless protected by WHOIS privacy.

b. Technical Data:

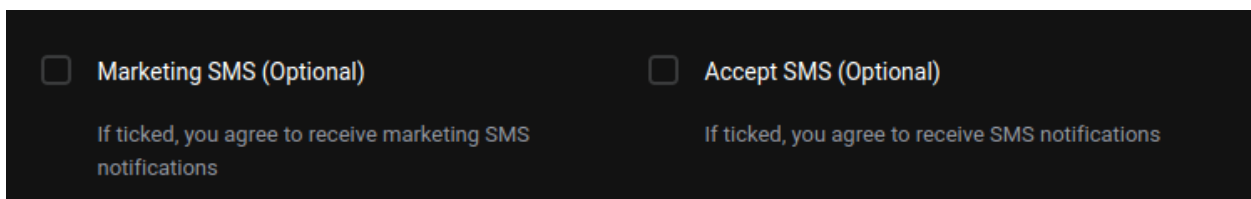
This is data related to the operation and performance of hosting services. Examples:

- **Access Logs:** IP addresses, login timestamps, and activity logs.
- **Hosting Statistics:** Bandwidth usage, server resource allocation, and uptime monitoring.

Legal Basis for Truehost's Data Processing

1. Consent Obtained During Account Creation and Service Use:

- Truehost collects explicit consent from users during account sign-up and service usage for specific purposes, such as receiving marketing emails or enabling optional services.
- See Example below attached.



Marketing SMS (Optional) Accept SMS (Optional)

If ticked, you agree to receive marketing SMS notifications If ticked, you agree to receive SMS notifications

2. Processing for Service Provision and Legitimate Interests:

- **Service Provision:** Data is processed as part of delivering core services like hosting, domain registration, Email hosting and DNS management and others.
- **Legitimate Interests:**
 - Preventing fraud.
 - Monitoring server health to ensure service quality.
 - Enforcing terms of service (e.g., identifying abusive activities).

Compliance Framework

Documenting Data Processing Activities

Maintaining a thorough record of data processing activities is a core compliance requirement for Truehost under the Kenya Data Protection Act (KDPA).

Key Components of a Data Processing Inventory:

1. Categories of Personal Data Collected:

- **Customer Account Information:** Names, email addresses, phone numbers, physical addresses, and billing details.
- **Payment Information:** Credit card or mobile money transaction details (e.g., M-Pesa).
- **Domain Registration Information:** Registrant details required for WHOIS records. (Captured during registration unless changed later)
- **Support Data:** Customer queries, chat logs, tickets and feedback for troubleshooting or service improvement.

2. Purpose of Processing Activities:

Each data category must have a documented and legitimate purpose, such as:

- **Account Management:** Storing customer data for user authentication, billing, and support.
- **Service Delivery:** Processing information required for domain registration, hosting setup, and DNS management.
- **Regulatory Compliance:** Retaining transaction records to comply with tax and financial regulations.
- **Marketing:** Sending promotional emails to users who have opted in.

3. Data Storage Locations: (Datacenter)

- Region based servers for hosting operations (e.g., in Europe, US, Kenya, South Africa, etc.).

4. Retention Periods:

- Personal data is retained only as long as it is necessary for the intended purpose. Examples:

- **Billing and Transaction Records:** Should be retained for 7 years to comply with financial reporting laws.
 - **Inactive Account Data(Expired Service):** Deleted after specified period as outlined in the terms of service policy.
-

2. Ensuring Data Minimization and Purpose Limitation

Truehost must ensure it processes only the minimum data necessary to achieve specific, lawful objectives. This principle reduces risk and improves compliance.

Data Minimization Practices:

1. Collecting Only Necessary Data:

- During account creation, Truehost limits required fields to essential information such as name, email address, and payment details and other important details required.
- Truehost avoids collecting unnecessary data such as personal identifiers (e.g., national IDs) .

2. Auditing Data Collection Forms:

- A regular review of all data entry points, such as:
 - Sign-up forms for hosting services.
 - Domain registration forms.
 - Servers Sign up forms
- Ensure optional data fields are clearly labeled and justified.

Purpose Limitation Practices:

1. Restricting Data Usage to Stated Purposes:

- Ensure customer data is used only for activities explicitly mentioned in Truehost's privacy policy.
Examples:
 - Using billing information strictly for payment processing.
 - Using email addresses for account-related communications or opted-in marketing campaigns.
- Prohibit using customer data for purposes outside of the agreed terms (e.g., selling user data to third parties).

2. Implementing Data Use Policies:

- Understanding by staff on the importance of adhering to these limitations.

Practical Compliance Checklist for Truehost's Services

To align with the Kenya Data Protection Act, Truehost ensures:

1. Transparency:

- It maintains a clear and accessible **privacy policy** outlining how personal and technical data is collected, processed, and stored.

2. Data Collection Practices:

- Obtains explicit consent for processing activities, especially for optional services.
- Provides opt-in and opt-out mechanisms for marketing communications.

3. Data Access Controls:

- Restricts access to personal data to authorized personnel only.
- Uses secure authentication protocols for system access.

4. Data Security Measures:

- Encrypts sensitive data (e.g., passwords).
- Regularly updates systems to ensure latest security patches.

5. Retention and Deletion Policies:

- Sets clear data retention timelines for shared hosting and VPS servers.
-