DATA PROTECTION & PRIVACY POLICY

Background

Data Protection (General) Regulations (DPR) is one of the regulations affecting the way that organizations carry out their information processing activities. It is the regulation that is designed to protect the personal data of Kenyan Citizens. Fines are applicable for any form of breaching DPR's rules and regulations. TFH must, therefore, ensure compliance with DPR by establishing a Data Protection & Privacy Policy.

Objective

The objective of this policy document is to describe TFH's responsibilities regarding the protection of personal data. It details our commitment to treat information of employees, customers, suppliers and any other stakeholders with care and confidentiality.

It is designed to ensure that TFH gathers, stores and handles data fairly, transparently, accurately, securely, with respect towards individual rights and the law, and is only held for as long as necessary for the purposes described.

Scope

This policy covers:

- board members
- all staff, including managers and supervisors; full-time, part-time or casual, temporary or permanent staff; job candidates; student placements; interns; apprentices; contractors and sub-contractors; and volunteers
- how TFH provides services to customers and suppliers and how it interacts with other members of the public
- all aspects of employment, recruitment, and selection; conditions and benefits; training and promotion; task allocation; shifts; hours; leave arrangements; workload; equipment and transport
- on-site, off-site or after work hours; work-related social functions; conferences – wherever and whenever staff may be because of their duties in TFH
- staff treatment of other staff, suppliers, customers and of other members of the public encountered in the course of their duties in TFH

TFH needs to gather and use certain information about individuals which can include (but is not limited to):

- Employees
- Customers
- Suppliers
- Business contacts

This policy applies to all data that the Company holds relating to identifiable individuals and to businesses, which includes (but is not limited to):

- Names of individuals
- Identity cards / passports / driving licenses
- Contact details including home / business addresses, email addresses and telephone numbers
- Next of kin details
- Bank accounts and financial details
- Statutory documents eg. NSSF details, NHIF details, Form P9 for PAYE, PIN Certificate
- Photos

- Medical records
- Names of spouse and children
- Biometric data
- Surveillance cameras (CCTV) etc
- HR records
- Financial transactions, including prices of goods and services
- Product specifications; details of processes or services; information regarding innovation
- Communications between TFH and individuals and other businesses

Purposes of holding data

These may include the following, or any other lawful purpose which we make the relevant stakeholder aware of:

- Making a decision about recruitment or appointment
- Determining the terms of employment
- Checking legal entitlement to work in KE
- Making payments and, for employees, deducting tax and any other lawful contributions
- Providing contractual benefits
- Liaising with pension providers
- Administering contracts
- Business management and planning, including accounting and auditing
- Conducting performance reviews, managing performance and determining performance requirements
- Making decisions about salary reviews
- Assessing qualifications for a particular job or task, including decisions about promotion
- Gathering evidence for possible grievance or disciplinary hearings
- Making decisions about continued employment or engagement
- Making arrangements for the termination of working relationships
- Education, training and development requirements
- Dealing with legal disputes involving employees, workers and contractors (including accidents at work) and with suppliers, customers, or any other stakeholders
- Ascertaining fitness to work
- Managing sickness absence
- Complying with health and safety obligations
- To prevent fraud
- To monitor the use of TFH information and communication systems to ensure compliance with its IT policies
- To ensure network and information security, including preventing unauthorised access to TFH computer and electronic communications systems and preventing malicious software distribution
- To conduct data analytics studies to review and better understand employee retention and attrition rates
- Equal opportunities monitoring
- To make business decisions on the procurement and supply of goods and services
- To monitor the timeliness of payments
- To ensure compliance with any legal requirements around the supply of goods or services
- To allow the compilation of data on the sustainability performance of TFH and its supplier base

Special categories of personal data

Personal Data- means any information relating to an identified or identifiable natural person.

Sensitive personal Data- means data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data (where used for ID purposes), property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination.

Data Protection risks

This policy helps to protect the Company from several types of data security risks, including:

- Breaches of confidentiality (for example, data being given out inappropriately)
- Failing to offer choice (for example, individuals should be free to choose how the Company uses data relating to them)
- Reputational or commercial damage (for instance, if hackers got access to data)

Security

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instruction and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Responsibilities

The Human Resources and Finance Managers have responsibility for the day-to-day implementation of this policy. Each team in TFH must ensure that data is handled and processed in line with this policy and data protection principles.

Principles

TFH will be guided by the principles of The Data Protection Act, 2019. These general principles are:

- **Lawful, fair and transparent**
  - Data collection must be fair, for a legal purpose and the Company must be open and transparent as to how the data will be used.
- **Limited for its purpose**
  - Personal data should be collected for specified and legitimate purposes.
- **Data minimization**
  - Any data collected must be necessary and not excessive for its purpose.
- **Accurate**

  - The data the Company holds must be accurate and kept up to date. Inaccurate personal data should be erased or rectified without delay.
- **Retention**
  - The Company cannot store data longer than necessary.
- **Integrity and confidentiality**
  - The data the Company hold must be kept safe and secure. Personal data should be processed and secured against any unlawful or unauthorized processing.

Rights of the Data Subject

The rights of the data subject under the DPR are:
- The right of being informed
- The right to access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The rights related to automated decision-making and profiling
- The right to object

Data subject rights are supported by appropriate procedures within TFH that allow the required action to be taken within the timescales stated under the DPR, as shown below:

Data Subject Request	Time scale
The right of being informed	Within one month (if the data is not supplied by the data subject)
The right to access	One month
The right to rectification	One month
The right to erasure	Without undue delay
The right to restrict processing	Without undue delay
The right to data portability	One month
The rights related to automated decision-making and profiling	Not specified
The right to object	On receipt of objection

Lawfulness of Processing

TFH's policy specifies the appropriate actions that should be taken for documenting and processing a specific case of personal data. However, DPR provides six alternative ways that can be used by TFH, depending on the case.

Consent

Except in specific reasons that are stated as allowable under DPR, TFH should obtain consent from the data subject, prior to collecting and processing their data. Consent can be oral, in writing and may include a handwritten signature, an oral statement or the use of an electronic or other medium to signify consent eg accepting terms & conditions, agreeing etc.

Contract performance

Explicit consent will not be required in cases where the collected and processed data are required for contract fulfillment, like cases when the contract cannot be finalized without the personal data. For example, if an address is missing in the delivery of a package, the delivery cannot be completed.

Legal obligation

Explicit consent will not be required in cases when the collected and processed data are required to comply with law. Taxation and employment can be examples of such cases.

Data subject's fundamental interests

A certain amount of data processing can be lawful under certain conditions (especially in the public sector), like cases when the data is needed to protect the subject's main interests or social care.

Carrying out tasks of public interest

The data subject's consent is not requested in cases where TFH needs to perform a specific task that is of public interest.

Legitimate interests

Data processing is considered lawful in cases when the processing of personal data does not significantly affect the rights and freedoms of the data subject. However, the taking of such actions should be justified properly and documented.

Data Protection by Design

TFH should adopt the principle of data protection by design and ensure that the systems collecting personal data consider privacy issues. The systems should also successfully complete one or more Data Protection Impact Assessment. The Data Protection Impact Assessment (DPIA) includes the following:

- Determine the purpose of processing the personal data
- Determine whether the processing of personal data is necessary
- Identify the necessary controls to address the risks and compliance with the legislation

In order to respect personal data privacy and compliance with DPR, TFH can use techniques, such as data minimization and pseudonymization. For data storage and safety in electronic devices (eg computers, phones, iPads, etc) TFH will ensure protection always for sensitive data by encrypting, anonymizing data so it cannot identify a person, that was it is safe if it were to leak.

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and give reference to any further regulations or retention timescales that may be relevant. TFH shall endeavor to conduct annual Data Protection Impact Assessment.

Processing Personal Data Contracts

Based on the requirements of DPR, TFH should ensure that all the personal data used are subject to a contract, i.e., the DPR Controller-Processor Agreement Policy.

Data Controllers and Data Processors will be bound by very strict policy on what they can do and what they cannot do, certificates shall be displayed conspicuously for audit purposes and professional conduct is key

Legitimate Purpose/Purpose Limitation

Any data collected or shared by an online service should only be done for a clear and specific purpose that is beneficial to the user. TFH should only collect user data for a specific purpose, clearly stating what that purpose is, and only retain data for as long as necessary to complete that purpose.

International Transfers of Personal Data

Before transferring any personal data outside of Kenya, TFH shall review and ensure that they comply with DPR regulations. Processing sensitive personal data outside the country will only be allowed after obtaining express consent from the Data Subject and after getting confirmation of appropriate security safeguards.

Therefore, in order to regulate the international data transfers, cross- border transfer agreements may be considered to provide enforceable rights for data subjects.

Limiting Transferability of Data

- Seek consent
- Explain in language well understood by the data subject
- Assurance that data will be used for the specified use, data is safe and secure
- Consent from Director of Public Prosecutions
- Recipient country should have equivalent Data Protection Law

Accountability and Transparency

TFH will ensure accountability and transparency in all its use of personal data and will show how it complies with each principle.
To comply with data protection laws and the accountability and transparency TFH shall endeavor to meet the following data protection obligations:

- Fully implement all appropriate technical and organizational measures
- Maintain up to date and relevant documentation on all processing activities
- Conduct Data Protection Impact Assessments
- Implement measures to ensure privacy by design and default, including data minimization, pseudonymisation & passwording, encrypting, and anonymising data so it cannot identify a person, that was it is safe if it were to leak
- Allowing individuals to monitor processing
- Creating and improving security and enhanced privacy procedures on an ongoing basis

Employer Responsibility

- Analysing and documenting the type of personal data the company hold
- Checking procedures to ensure they cover all the rights of the individual
- Identify the lawful basis for processing data
- Ensuring consent procedures are lawful
- Implementing and reviewing procedures to detect, report and investigate personal data breaches
- Store data in safe and secure ways
- Assess the risk that could be posed to individual rights and freedoms should data be compromised
- Register data processors & controllers
- Report any breach of the regulations

Employee Responsibility

- Fully understand your data protection obligations
- Check that any data processing activities you are dealing with comply with our policy and are justified
- Do not use data in any unlawful way
- Do not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and the company policies through your actions
- Comply with this policy at all times
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay

Third Parties

TFH will have written contracts in place with any third-party Data Controllers and/or Data Processors that the Company may use. The contract must contain specific clauses which set out our and their liabilities, obligations and responsibilities.

TFH must only appoint processors who can provide sufficient guarantee that the rights of data subjects will be respected and protected

Criminal Record Checks

Any criminal record checks must be justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject. The Company cannot keep a comprehensive register of criminal offence data. All data relating to criminal offences is considered to be a special category of personal data and must be treated as such. You must have approval from the Legal Officer prior to carrying out a criminal record check.

Reporting Breaches

The objective of this policy is to contain any breaches, minimize the risk associated with any breaches and consider what action is necessary to secure personal data and prevent further breaches.

Any breach of this policy or of relevant data protection laws must be reported to the Office of Data Protection (Office of the Director of Public Prosecutions) as soon as practically possible. This means as soon as you have become aware of a breach, whether by yourself, temporary staff, casual staff,

contractors, consultants, suppliers or data processors or controllers or any other person or body working for or with the company, TFH has a legal obligation to report any data breaches to the relevant supervisory or statutory authority within 72 hours.

A breach means an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to the Company's information assets and/or reputation. This includes (but is not restricted to) the following:

- Loss or theft of confidential or sensitive data or equipment on which such data is stored (eg loss of laptop, USB stick, iPad/tablet device, or paper record)
- Equipment theft or failure
- Unauthorized use of access to or modification of data or information systems
- Attempts (failed or successful) to gain unauthorized access to information or IT system(s)
- Unauthorized disclosure of sensitive / confidential data
- The Company site defacement
- Hacking attack
- Unforeseen circumstances such as a fire or flood
- Human error
- 'Bragging' offences where information is obtained by deceiving the organization who holds it

In event of a breach (e.g. hacking), it is TFH's responsibility to notify the office of Data Protection (Office of the Director of Public Prosecutions), clearly stating date, circumstances of breach, steps to mitigate, ensure you tell the office potential harm to the employee, demonstrate how secure your system is / integrity of the system, who has access both physical and electronic & security or safety of data.

Disciplinary Consequences

All principles described in this policy must be strictly followed. A breach of data protection guidelines will invoke disciplinary up to and including summary dismissal and possibly legal action.

Review of the Policy

This policy shall be reviewed annually by the Human Resources Manager and Chief Finance Officer in consultation with TFH's Management team.

(Signed)

Director

30th October 2024