

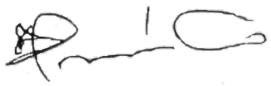



Guaranty Trust Pension Managers

# **GUARANTY TRUST PENSION MANAGERS LIMITED**

---

## **DATA PROTECTION POLICY**

<b>Title</b>	<b>Guaranty Trust Pension Managers Limited Data Protection Policy</b>		
<b>Date Created</b>	<b>December 20, 2022</b>		
	<b>Title</b>	<b>Signature</b>	<b>Date</b>
<b>Prepared by</b>	<b>Head, Compliance</b>		December 20, 2022
<b>Reviewed by</b>	<b>Managing Director/CEO</b>		January 19, 2023
<b>Approved by</b>	<b>Board</b>	Approved	January 20, 2023
<b>Classification</b>	Internal		
<b>Reference</b>	NDPR 2019; EU GDPR (2016/679); Capital Market Operators AML/CFT Regulations, 2022; Central Bank of Nigeria AML/CFT/CPF Regulations 2022, Section 35 & 36; GTPension Data Privacy Policy		
<b>Summary</b>	Policy detailing how the organization ensures all data is protected		
<b>Version</b>	1.0		

## Table of Contents

<b>Introduction</b> .....	4
<b>Purpose</b> .....	4
<b>Scope</b> .....	5
<b>Definitions</b> .....	5
<b>Details</b> .....	6
<b>Employee Data</b> .....	7
<b>Data Subjects' Rights</b> .....	7
<b>Consent and other Lawful Basis</b> .....	9
<b>Responsibility</b> .....	10
<b>Protection of Data</b> .....	11
<b>Data Life Cycle and Retention of Data</b> .....	11
<b>Data Breach</b> .....	13
<b>Third Party Processing and Transmission of Data</b> .....	13
<b>Compliance</b> .....	15
<b>End User Security</b> .....	15
<b>Review</b> .....	16

## Introduction

Guaranty Trust Pension Managers Limited ("GTPension") holds and processes information about customers, employees, and other data subjects for administrative, operational and commercial purposes. It may also process such information to fulfil legal obligations and contractual agreements. When handling such information, GTPension staff or others who process or use any personal information must comply with the Data Protection Principles.

In summary, this states that personal data shall:

- ✚ be processed fairly, lawfully and in a transparent manner.
- ✚ be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with such purposes.
- ✚ be adequate, relevant and limited to what is necessary to fulfil the purpose of processing.
- ✚ be accurate and where necessary, up to date. In the event that data is inaccurate, steps should be taken to rectify or erase such data.
- ✚ not be kept for longer than necessary for the purpose of processing.
- ✚ be processed in accordance with the data subject's rights.
- ✚ be kept safe from unauthorized processing, and accidental loss, damage or destruction using adequate technical and organizational measures.

## Purpose

GTPension takes protection of data collected or processed by it very seriously. The aim of this policy is to ensure that GTPension applies best practice in protecting data at rest, in use and during transmission from unauthorized access, disclosure, modification or destruction as well as meet regulatory and stakeholder requirements with respect to the protection of data.

## Scope

This Policy applies to all staff of GTPension including permanent or contract, agency staff, sub-contracted staff, volunteers or interns. All third parties that process data on behalf of GTPension are also expected to comply with this Policy.

## Definitions

**"Data controller"** is a person (natural or legal) who (either alone or jointly or in common with other persons) determine the purposes for which and the manner in which any personal data are processed.

**"Staff"** refer to current employees of GTPension. This includes permanent or temporary, full or contract staff, agents, interns, third-party representatives or sub-contractors.

**"Data subjects"** are identifiable or identified natural persons.

**"Data Processor"** refers to any entity (natural or legal) that is authorized by the data controller to process personal data. This may include contractors, suppliers, vendors and other service providers.

**"Data Protection Officer"** is an individual given the mandate by GTPension to oversee its data protection implementation and compliance with national and international data protection regulations.

**"Processing"** refers to any action or set of actions performed on personal information, including obtaining, organizing, and viewing, copying, modifying, amending, adding, deleting, extracting, sharing, storing, disclosing or destroying information.

**"Consent"** refers to any freely given, explicit, clear and informed indication of a data subject's agreement to the processing of his/her personal data.

**"Data breach"** refers to a breach of security that results in an accidental, unauthorized or illegal access, disclosure, modification, loss, transmission or destruction of data.

**"Sensitive Information"** refers to all types of data that must be protected from unauthorized access to safeguard the privacy or security of an individual or organization. It includes Personally Identifiable Information (PII), authentication credentials, card data, transaction information etc. This list is not exhaustive.

**“Highly Sensitive Data”** refers to information about a data subject’s health, ideological beliefs, origin including race or ethnicity, sexual orientation, biometric information.

## Details

### Staff Responsibilities

#### Information provided by Staff to GTPension

All staff shall:

- ✚ Ensure that all personal information which they provide to GTPension in connection with their employment is accurate and up to date.
- ✚ Inform GTPension of any changes to information, for example, changes of address.
- ✚ Check the information which GTPension shall make available from time to time, in written or automated form, and inform GTPension of any errors; where appropriate, follow laid down procedures for updating entries.  
GTPension shall not be held responsible for errors on which it has not been informed.

#### Information held or processed by staff

Staff are to apply due care and due diligence in processing information held by GTPension. All staff are expected to properly classify information (refer to Information Classification Policy) into categories determined by GTPension and handle such information with appropriate care. In particular, care of customer data should be taken very seriously. Staff shall ensure that:

- ✚ All personal information is stored securely.
- ✚ You shall only take data sufficient for your need.
- ✚ You shall only hold data for the minimum time required to complete your work.
- ✚ You shall destroy data when no longer required and confirm to the client this has been done.

- ✦ You shall not share data with third parties except expressly authorized by the customer and approving authority within GTPension.
- ✦ Only information that you are authorized to access shall be processed by you.
- ✦ Personal information in any form (including visual, verbal, written, electronic or any other media or manner) is not to be disclosed accidentally or otherwise to any unauthorized third party. Unauthorized disclosure may be a disciplinary matter and may be considered gross misconduct in some cases.
- ✦ Due care must be exercised by staff when processing sensitive data.

## Employee Data

Over the course of the employment relationship, including application to terminate the employment agreement, personal data of the data subject concerned can be processed to initiate or fulfil the terms of the employment contract. If the personal data of an employee is required for a purpose not covered in the employment contract, consent must be obtained from the data subject in relation to that purpose except in the cases where this is a legal or regulatory requirement or such processing is in the vital interest of a natural person.

Agreement to GTPension processing some specified classes of personal data is a condition of employment for staff. Such data is necessary for the initiation, execution or termination of the employment contract.

## Data Subjects' Rights

Data subjects shall have the right to access any personal data that is being kept about them whether it is held on an electronic device or in physical files. This right may be exercised by submitting a request in writing to the appropriate designated data controller or to the data protection officer. In the event that the request is submitted to the DPO, the DPO is to ensure that such request is forwarded to the relevant designated data controller for treatment.

GTPension aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 48 hours unless there is

good reason for delay. In such cases, the reason for the delay shall be explained in writing by the designated data controller to the data subject making the request.

Data subjects have the right to receive their personal data that they have provided to GTPension in a structured, commonly used and machine-readable format where:

- Processing is based on consent or on a contract;
- Processing is carried out via automated means.

Where technically feasible (and subject to administrative costs), the data subjects have the right to request that such data be transmitted to another controller, provided that this right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller. In the event such request cannot be addressed, response should be provided to the data subject as quickly as possible.

In the cases of inaccurate data, data subjects have the right to request that such data be rectified. Taking into account, the current state of technology, as well as the type of information that needs to be rectified, data subjects can exercise such rights through the appropriate customer touch points of GTPension.

Data subjects have the right to request that processing of their personal data be restricted. GTPension reserves the right to honor this request subject to regulatory requirements or legitimate interests of GTPension.

Data subjects have the right to request that their data be deleted. This request should be in writing to the designated data controller (see definition below). GTPension reserves the right to honor this request subject to regulatory requirements for the retention of data and other operational needs or legitimate interests of GTPension. If the request is refused, the decision will be communicated to the data subject.

For more description of data subjects' rights, refer to GTPension's **Privacy Policy**.



## Consent and other Lawful Basis

When handling sensitive information or processing research data, GTPension does not process personal data without the explicit consent of the individual unless as stated in this policy. Consent may not be required when there are valid reasons. These include the various lawful basis for processing of personal data below:

- ✚ Cases where processing of personal data is required for the fulfilment of a contractual obligation entered into by the data subject.
- ✚ Cases where processing of personal data is required for compliance with legal and/or regulatory requirements.
- ✚ Cases where processing is required to protect the vital interest of the data subject or any other natural person.
- ✚ Cases where processing is required for an activity to be carried in significant public interest.
- ✚ Cases where processing is required for legitimate interests of GTPension or a third party insofar as this does not conflict with the requirements for the protection of personal data of a data subject.

These lawful bases provide the underlying support for the processing of personal data by GTPension.

Prior to the collection of consent, the data subject should be made aware of the identity of the data controller (here GTPension), the purpose(s) for the collection of data and the categories of third parties whom the data might be shared with. All of these are available on GTPension's Privacy Policy. A privacy notice which abridges GTPension's comprehensive Privacy Policy can be provided to the data subject at such data collection points.

Consent can be given via electronic or written means. In the event that the data subject is not directly present when giving consent, technical, administrative and other measures must be put in place to confirm/prove the identity of the data subject.

Consent already given can also be withdrawn by the customer. Withdrawal of

consent can be made via writing to the designated data controller. If consent is withdrawn, the data of the customer should no longer be processed unless there exists another lawful basis by which the data can be processed. If there are multiple purposes of processing of the data, the data cannot be processed for the purpose in which consent has been withdrawn. Withdrawal of consent does not affect the lawfulness of processing prior to such withdrawal.

GTPension may process sensitive information about a person's health, disabilities, criminal convictions, race or ethnic origin in pursuit of the legitimate interests of GTPension. GTPension may also require such information for the administration of the HR staff policy, or for internal review.

GTPension may also ask for information about particular health needs, such as allergies to particular forms of medication, or conditions such as asthma or diabetes. GTPension will only use such information to protect the health and safety of the individual, for example, in the event of a medical emergency. The consent of the data subject will always be sought prior to the collection of any sensitive data.

### **Consent for Minors (Children below 18 years)**

---

In cases where the data subject is a minor, consent can only be given by the parents or legal guardians of the data subject otherwise processing of the personal data is not considered lawful.

This requirement can only be waived subject to a regulatory approval.

## **Responsibility**

The Management Board of Directors of GTPension are the data controllers, and the process owner is ultimately responsible for implementation. Responsibility for day-to-day matters will be delegated to the Heads of Department as designated data controllers.

The Data Protection Officer (DPO) oversees the data protection efforts including strategy, compliance advisory, and implementation recommendations and

assists to coordinate the data protection activities for GTPension.

Information and advice about the holding and processing of personal information shall be made available by the DPO.

## Protection of Data

Personal data including all sensitive information should be adequately protected in storage, transit and in use from unauthorized disclosure (both internal and external) or processing using state of the art technical and organizational measures. Such practices should be introduced at every stage of the data lifecycle as current technology and operational realities allow.

This applies whether sensitive information exists in physical or electronic form. Of particular note is information used to authenticate an object (user/customer/system/application) executing a business transaction. This includes PIN, password, passcode, One-time transaction code and secret answer. These items must be encrypted in line with the requirements of the cryptographic policy except where a business justification exists. Access to sensitive data should be restricted to authorized staff.

Before the introduction of any service, process or product that processes data (especially those involving information technology), techniques (of an organizational and technical measure) that protect this data from unauthorized disclosure, use or transmission must be defined and implemented. In relation to personal data, these include assessments to ensure that the data to be collected is necessary for the processing that is to be carried out in order to meet data minimization requirements.

## Data Life Cycle and Retention of Data

Data processed by GTPension follows a life cycle. This refers to the steps from the creation/collection of data to its destruction/disposal. Taking into consideration factors such as the current state of technology, the cost, legal & regulatory

requirements, at every step of the data life cycle (creation/collection, preparation, storage, use, archival and disposal), data should be protected by technical and organizational measures that ensure the confidentiality, integrity and availability of data.

After activities such as collection/creation, preparation and usage, some data may have to be stored for re-use or archival purposes. The periods for retention of data depends on legal and operational requirements. In line with the data protection principles, data should be retained no longer than it is required for the purposes of supporting business operations. In particular, staff should ensure that personal data is not kept on their endpoints for a period longer than what is designated for processing.

The means for retention of data shall account for the form which data is held (paper, electronic), the cost of storage, current state of technology and legal & regulatory requirements.

Personal data is retained in accordance with our data retention policy. We abide by the minimum regulatory requirements and extant laws in our operating environment. We keep this data:

- For as long as there is an ongoing business relationship with the data subject
- For as long as required to fulfil our legal, regulatory, tax and other business obligations
- In most cases for a period of at least 5 years after the end of a relationship

#### References

1. GDPR 2019: Implementation Framework – Retention of Records (Art. 2.1(1c) GDPR)
2. Central Bank of Nigeria AML/CFT/CPF Regulations 2022, Section 35 & 36
3. Securities & Exchange Commission (Capital Market Operators AML/CFT Regulations, 2022)

## Data Breach

When a data breach has been discovered, the relevant regulatory authorities have to be notified by GTPension of the breach. Such disclosure should be carried out within 72 hours of the discovery of the breach. In cases where the breach is likely to result in losses and/or harm to the data subject, GTPension should inform him/her of such breach within a reasonable timeframe.

The responsibility for reporting a suspected breach lies with the person who discovered the breach. Breaches should be reported to the DPO, who then takes it up with the appropriate quarters. Breaches should be reported once detected as the longer a breach remains undetected, the greater the risks to GTPension as well as other entities whose data have been compromised.

Breaches may occur from one of the following sources:

- ✚ Loss or theft of data or medium containing data
- ✚ Human error e.g. unintended transmission/disclosure of data to wrong party
- ✚ Malicious actors (internal & external)
- ✚ Insecure disposal of information (e.g. not shredding documents, simple deletion of sensitive files)
- ✚ Inadequate access controls
- ✚ Password compromise
- ✚ Software/hardware errors
- ✚ Security misconfiguration

All employees are required to report any suspected cases of breach arising from any of the previously noted sources.

## Third Party Processing and Transmission of Data

All third-party processing of personal data must be governed by a written contract/agreement. This agreement can be stand-alone or part of the SLA/contract/service order or any other binding agreement and should lay the

terms for the processing of data. Please contact the Legal team for review of such documents. At a minimum, such contract/agreement must contain the rights and obligations of both parties with respect to the processing of personal data and should address the following:

- ✚ Compliance with applicable data protection laws, requirements & regulations in processing personal data and assistance with information that demonstrates compliance where needed.
- ✚ Terms of processing i.e. processing of personal data should be carried out based strictly on the controller's documented instruction.
- ✚ Nature and purpose(s) of processing.
- ✚ Appropriate technical and administrative measures to ensure that personal data is processed securely in accordance with security and privacy best practices.
- ✚ Appropriate technical and administrative measures to assist GTPension in responding to requests from data subjects or relevant authorities with respect to data privacy.
- ✚ Data breach response measures including notification timelines (without undue delay) to GTPension in the event of a data breach.
- ✚ Right to audit clauses with respect to the third party's data processing activities.
- ✚ Handling of data after processing is completed including after end of contract.
- ✚ Rules of engagement with sub-processors/contractors.

Transfer of data inside and outside of GTPension is subject to necessary approvals and authorizations obtained. Data must only be used for the purpose(s) defined. Employees and teams entering into agreements with third parties that involve the transfer of personal data outside GTPension should at a minimum have a data processing agreement with the said third party.

If data is to be transmitted outside of GTPension to a third party, there must be assurance provided by that third party that it would take adequate technical and organizational measures in protecting the data and that such data would only be used for the intended purposes.

Data transfer outside of Nigeria to any country must comply with extant data privacy regulations regarding the transfer of data outside the country. In principle, cross border personal data transfer can be processed when the recipient can indicate that it can provide data protection compliance that is equivalent to this Data Protection Policy or meets industry best practice. Otherwise such data transfer will be subject to laid provisions for exceptions to transfer of personal data in extant data privacy regulations.

## Compliance

Compliance with Data Protection is the responsibility of all members of staff and all partners that process personal data controlled/processed by GTPension. Any deliberate or reckless breach of this Policy may lead to disciplinary, and where appropriate, legal proceedings. Any questions or concerns about the interpretation or operation of this policy should be sent to GTPension's Data Protection Officer (DPO) via [DPO@gtpensionmanagers.com](mailto:DPO@gtpensionmanagers.com).

Any individual, who considers that the policy has not been followed in respect of personal data about him or herself, shall first raise the matter with the Designated Data Controller. If the matter is not resolved it shall be treated in line with the staff grievance or complaints procedure.

## End User Security

### **Data processed on Employee Devices**

Whether end users are using desktop or laptop PCs, there is a risk that data can be lost due to hardware failure or user error. Staff must accept responsibility for the machines they use and ensure that data is regularly backed up to minimize loss to the business as a result of such events.

Where classified information must be processed on a portable computer in an area where not all personnel are cleared or have a "need to know" status, you

shall take due care in ensuring that such data is protected from unauthorized access, disclosure, use or modification for example position the computer carefully to avoid casual overview, locking your system when not in use etc.

Products for secure access control, secure transmission, endpoint protection and hard-disk encryption are recommended for laptops that contain classified information and may be taken outside the organization. GTPension already employs software to carry this out and deems it necessary to have these measures in place.

## **Review**

This is policy shall be reviewed every three (3) years to reflect current realities and such reviews must be presented for adoption and approval by the Board.