VETIVA

DATA PROTECTION POLICY

1. Introduction

Vetiva Capital Management Limited (including its subsidiaries Griffin Finance Limited, Vetiva Advisory Services Limited, Vetiva Fund Managers Limited, Vetiva Securities Limited and Vetiva Trustees Limited, hereinafter collectively referred to as "Vetiva"), as a data collector/controller, is committed to conducting its business in accordance with the Nigeria Data Protection Regulation (NDPA), EU General Data Protection Regulation (GDPR), and other international instruments concerning the protection of personal data and privacy of individuals privacy to ensure compliance with the Data Protection requirements. Non-compliance may expose Vetiva to complaints, regulatory actions, fines or/and reputational damage.

2. Purpose

The purpose of this policy is to ensure that Vetiva processes personal data in a way that is consistent with all data protection and privacy guidelines, to protect the "rights and freedoms" of individuals, and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

Vetiva's Data Protection Policy is also designed to inform all stakeholders about their obligation to protect the privacy and security of personal data when collecting, storing, using personal data that is needed in order to carry out our business while complying with Data Protection Regulations and standards.

3. Rational/Scope

By this policy, Vetiva sets forth how it shall process and manage personal data collected in the normal course of business. Any data provided are handled in a confidential manner to ensure that the content and service being offered are tailored to specific requests, needs and interests.

Vetiva's policy applies to all employees, contractors, vendors and third parties that are responsible for processing of personal data on behalf of Vetiva.

This policy also applies to the whole or part processing of personal data by automated means (i.e. by laptop/computer) and non-automated means (i.e. paper records) that form part or intend to form part of Vetiva's filing system.

4. Definition of Terms

Personal Data – A name, identification number, location data, and/or online identifier, including one or more specific factors such as physical, physiological, genetic, mental, economic, cultural or social identifiers relating to a natural person directly or indirectly.

Data Subject – Any living individual or natural person from whom personal data is collected.

Consent - Any specific, informed, and unambiguous indication of the data subject's wishes that is freely given by a statement or by a clear affirmative action, which signifies agreement to the processing of his/her personal data.

Third Party – A natural or legal person, public authority, agency, vendor, contractor, or entity other than the data subject, who, under Vetiva's authority, is authorised to process personal data.

Data Administrator – Any persons or organisation that processes data.

Data Controller - Any person who either alone, jointly with other persons or in common with other persons or as a statutory body, determines the purposes for and the manner in which personal data is processed or is to be processed.

Processing - Any operation or set of operations which is performed on personal data or on sets of personal data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Protection Impact Assessment - A tool and process for assessing the protection impacts on data subjects in processing their personal data and for identifying remedial actions as necessary in order to avoid or minimize such.

Data Protection Officer – A Vetiva staff who supervises, monitors and reports matters related to data protection and privacy in compliance with this Policy.

Data Encryption – The process of converting data or information into a code to prevent unauthorised access by human and/or computer systems. Data encryption can be used during data storage or transmission and is typically used in conjunction with authentication services to ensure that keys are only provided to, or used by, authorized users.

Personal Data Breach - A breach of data security leading to the accidental or unlawful/illegitimate access, destruction, loss, alteration, unauthorized disclosure of personal data that is being transferred, stored or otherwise processed.

5. Policy Statement & Applicability

The entire Management Board of Vetiva, located at Plot 266B Kofo Abayomi street, Victoria Island, Lagos, is committed to maintaining compliance with all relevant GDPR/NDPA and local laws with respect to personal data collected, as well as protection of the "rights and freedoms" of the data subject. This GDPR/NDPA compliance policy is also described by other relevant policies such as the information security policy, along with related Vetiva processes and procedures.

The GDPR/NDPA and Vetiva's data protection policy applies to all personal data processing functions, including those performed on customers', clients', employees', suppliers' and partners' personal data, and any other personal data that Vetiva processes from any source. This policy also applies to all Employees/Staff and third parties of Vetiva.

Vetiva's Data Protection Officers are responsible for reviewing and updating the register of processing annually in the light of any changes to Vetiva's operations and activities, and to any additional requirements identified by means of data protection impact assessments. This register needs to be available on the supervisory authority's request.

Partners and any third parties working with or for Vetiva, and who have or may have access to personal data, will be expected to have read, understood, and to comply with this policy. No third party may access personal data held by Vetiva without having first entered into a Data Confidentiality/Non-Disclosure Agreement, which imposes on the third-party obligations no less onerous than those to which Vetiva is committed, and which gives Vetiva the right to audit compliance with the agreement.

Any breach of the GDPR/NDPA will be dealt with under Vetiva's disciplinary procedure and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

6. Roles & Responsibilities

Roles	Responsibilities
Management, CEO, Supervisors	• Develop and encourage good information handling practices within Vetiva; responsibilities are set out in individual job descriptions.
Data Protection Officers	• Are accountable to Vetiva's Management Board for the management of personal data within Vetiva. • Ensure that compliance with data protection legislation and good practice can be demonstrated. • Are accountable for development and implementation of the GDPR/NDPA as required by this policy. • Are accountable for security and risk management in relation to compliance with the policy.
Employees/Staff	• Ensure that any personal data about them and supplied by them to Vetiva is accurate and up-to-date.

Under the GDPR/NDPA, Vetiva is a ***data controller and/or data processor***.

The Data Protection Officers, who the Management Board consider to be suitably qualified and experienced, have been appointed to take the responsibility for Vetiva's compliance with this policy on a daily basis.

The Data Protection Officers have specific responsibilities in respect of procedures such as the Subject Access Request Procedure and are the first point of call for Employees/Staff seeking clarification on any aspect of data protection compliance.

Compliance with the Nigerian Data Protection Act is also the responsibility of all Employees/Staff of Vetiva who use/process personal data. Vetiva's Training Policy sets out specific training and awareness requirements in relation to specific roles and Employees/Staff of Vetiva generally.

7. Data Protection Principles

All personal data collection, processing, retention, transfer, disclosure and destruction are conducted in accordance with the GDPR/NDPA data protection principles. Vetiva's policies and procedures are also designed to ensure compliance the following principles, as listed below;

7.1 Lawful, Fair, and Transparent Processing of Personal Data

Processing of personal data may only be carried out on a legitimate basis and in a fair and transparent manner. In order to process data of individuals lawfully, fairly, and transparently, Vetiva shall ensure to seek consent from data subjects as the primary condition for processing.

Vetiva processes personal data to ensure the safety and security of persons of concern or other individuals.

Whether the data is obtained from the data subjects directly or indirectly, Vetiva ensures that certain information are available to the data subjects as practicable, according to Vetiva's Transparency Requirement. Data subjects are also given an easily understandable and accessible privacy information notice, including other specific necessary information like;

i. the contact details of the Data Protection Officer;
ii. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
iii. the period for which the personal data will be stored;
iv. the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights;
v. the categories of personal data concerned;
vi. the recipients or categories of recipients of the personal data, where applicable;
vii. where applicable, that the controller intends to transfer personal data to a recipient in a foreign country and the level of protection afforded to the data;
viii. any further information necessary to guarantee fair processing.

7.2 Collection of Personal Data Only for Specific, Explicit, and Legitimate Purposes

Data obtained are for specified purposes, and will not be used for any purpose that differs from those formally notified to the data subject and supervisory authority as set out by Vetiva's GDPR/NDPA register of processing and privacy procedure.

7.3 Necessity & Data Minimization

Personal data collected by Vetiva shall be adequate, relevant and limited to what is necessary for processing. This means that Vetiva's Data Protection Officers are responsible for ensuring that only information that is strictly necessary is obtained. All forms of data collection (electronic or paper-based), including data collection requirements in new information systems, will include a fair processing statement or link to privacy statement, and approved by the Data Protection Officers.

The Data Protection Officers will ensure that all data collection methods are reviewed annually to ensure that collected data continues to be adequate, relevant and not excessive.

7.4 Accurate, Easy Rectification, and Deletion

Personal Data shall be accurate and kept up to date. All personal data stored by Vetiva must be reviewed and updated as necessary to ensure that data is accurate and up-to-date. No personal data shall be kept unless it is reasonable to assume that it is accurate, and the Data Protection Officers are responsible for ensuring that all Vetiva staff are trained in the importance of collecting accurate personal data and maintaining it.

The data subject must ensure that any data held by Vetiva is accurate and up-to-date. Completion of electronic or hard copy forms by a data subject will include a statement that the data contained therein is accurate at the date of submission.

Employee/Staff/Customers/Clients and other data subjects are required to notify Vetiva of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of Vetiva to ensure that any notification regarding change of circumstances is recorded and acted upon.

The Data Protection Officer is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

On at least an annual basis, the Data Protection Officer reviews the retention dates of all the personal data processed by Vetiva and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted/destroyed in line with the Secure Disposal of Storage Media Procedure.

The Data Protection Officer is responsible for responding to requests for rectification from data subjects within one month (Subject Access Request Procedure). This can be extended to a further two months for complex requests. If Vetiva decides not to comply with the request, the Data Protection Officer must respond to the data subject to explain its reason and inform them of their right to complain to the supervisory authority and seek judicial remedy.

The Data Protection Officer is responsible for making appropriate arrangements that, where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.

7.5 Storage Limitation

Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing. Where personal data is to be retained beyond the processing date, it will be encrypted in order to protect the identity of the data subject in the event of a data breach.

Personal data will be retained in line with the Retention of Records Procedure. Once this retention date is passed, it shall be securely destroyed as set out in this procedure.

The Data Protection Officer must, in written form, specifically approve any data retention that exceeds the retention periods defined in Retention of Records Procedure, and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation.

7.6 Integrity and Confidentiality

Personal data shall be processed in a manner that ensures appropriate security of personal data including protection against unauthorized and unlawful processing, accidental loss, destruction, or damage. Vetiva shall use appropriate technical and organizational measures to ensure the integrity and confidentiality of personal data is maintained at all times.

In determining appropriateness, the Data Protection Officer should also consider the extent of possible damage or loss that might be caused to individuals (staff/customers) if a security breach occurs, the effect of any security breach on Vetiva itself, and any likely reputational damage including the possible loss of customer trust.

When assessing appropriate technical measures, the Data Protection Officer will consider the following:

i. Password protection;
ii. Automatic locking of idle terminals;
iii. Removal of access rights for USB and other memory media;
iv. Virus checking software and firewalls;
v. Role-based access rights including those assigned to temporary staff;
vi. Encryption of devices that leave the organisations premises such as laptops;
vii. Security of local and wide area networks;
viii. Privacy enhancing technologies such as pseudonymisation and anonymisation;
ix. Identifying appropriate international security standards relevant to Vetiva.

When assessing appropriate organisational measures, the Data Protection Officer will consider the following:

i. The appropriate training levels throughout Vetiva;
ii. Measures that consider the reliability of employees (such as references etc.);
iii. The inclusion of data protection in employment contracts;
iv. Identification of disciplinary action measures for data breaches;
v. Monitoring of staff for compliance with relevant security standards;
vi. Physical access controls to electronic and paper-based records;
vii. Adoption of a clear desk policy;

viii. Storing of paper-based data in lockable fire-proof cabinets;
ix. Restricting the use of portable electronic devices outside of the workplace;
x. Restricting the use of employee's own personal devices being used in the workplace;
xi. Adopting clear rules about passwords;
xii. Making regular backups of personal data and storing the media off-site;
xiii. The imposition of contractual obligations on the organisation to take appropriate security measures when transferring data to foreign countries.

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

7.7 Accountability

Vetiva shall be able to explicitly demonstrate compliance with accountability and governance, as well as all other GDPR/NDPA data protection principles by implementing data protection policies, adhering to codes of conducts, implementing technical and organizational measures, and adopting techniques such as Data Protection by design, Data Protection Impact Assessments (DPIAs), breach notification procedures, and incidence response plan.

8. Rights of the Data Subject

As regards data processing and recording, data subjects have the right to:

i. Be informed of the specific purpose for which the personal data will be processed, and if the data will be transferred or disclosed to a third party.
ii. make subject access requests regarding the nature of information held and to whom it has been disclosed.
iii. prevent processing likely to cause damage or distress.
iv. prevent processing for purposes of direct marketing.
v. be informed about the mechanics of automated decision-taking process that will significantly affect them.
vi. not have significant decisions that will affect them taken solely by automated process.
vii. sue for compensation if they suffer damage by any contravention of the GDPR/NDPA.
viii. take action to rectify, block, erase, including the right to be forgotten, or destroy inaccurate data.
ix. request the supervisory authority to assess whether any provision of the GDPR/NDPA has been contravened.
x. have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.
xi. object to any automated profiling that is occurring without consent.

Vetiva also ensures that:

i. Data subjects may make data access requests as described in Subject Access Request Procedure; this procedure also describes how Vetiva will ensure that its response to the data access request complies with the requirements of the GDPR/NDPA.

ii. Data subjects have the right to complain to Vetiva relating to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled in line with the Complaints Procedure.

9. Consent

Vetiva understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.

Vetiva understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

There shall be some active communication between the parties to demonstrate active consent. Consent shall not be inferred from non-response to a communication and Vetiva must be able to demonstrate that consent was obtained for the processing operation.

For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

In most instances, consent to process personal and sensitive data is obtained routinely by Vetiva using standard consent documents e.g. when a new client signs a contract, or during induction for participants on programmes.

Where Vetiva provides online services to children, parental or custodial authorisation must be obtained. This requirement applies to children under the age of 16 in the case of GDPR and 18 in the case of NDPA.

10. Data Security

For security of personal data;

- All Employees/Staff are responsible for ensuring that any personal data that Vetiva holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by Vetiva to receive that information and has entered into a confidentiality agreement.
- All personal data shall be accessible only to those who need to use it, and access may only be granted in line with the Access Control Policy. All personal data shall be treated with the highest security and must be kept:
    i. in a lockable room with controlled access; and/or
    ii. in a locked drawer or filing cabinet; and/or
    iii. if computerised, password protected in line with corporate requirements in the Access Control Policy; and/or
    iv. stored on (removable) computer media which are encrypted in line with Secure Disposal of Storage Media.

Care must be taken to ensure that PC screens and terminals are not visible except to authorised Employees/Staff of Vetiva. All Employees/Staff are required to enter into an Acceptable Use Agreement

before they are given access to organisational information of any sort, which details rules on screen time-outs.

Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit written authorisation.

Personal data may only be deleted or disposed of in line with the Retention of Records Procedure. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed as required by before disposal.

Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site.

Contracts with second-level subcontractors will only be approved if they are required to comply with at least the same security and other provisions as the primary subcontracting organisation (the vendor/supplier) if the subcontractor specify that, when the contract is terminated or upon the request of the data subject on legal grounds, related personal data will either be destroyed or returned to Vetiva, and so on down the chain of sub-contracting.

10.1 Data Encryption

Data Encryption is the process of converting data or information into a code to prevent unauthorised access by human and/or computer systems. Data encryption can be used during data storage or transmission and is typically used in conjunction with authentication services to ensure that keys are only provided to, or used by, authorized users.

It is the policy of Vetiva to protect sensitive data or asset from unauthorized access (whether stored on a system within the office environment or on other location, or in transit) by the use of encryption technologies.

Procedure.

- Data Storage Devices

All personal data storage devices that are owned by Vetiva or contains data related to Vetiva shall be encrypted.

Examples of data storage devices are, but not limited to: Laptops, Desktop Computers, USB Flash Drives, External Hard Drives, Smartphones, etc.

- Encryption Administration

- Vetiva IT shall ensure that all portable data storage devices purchased or in use, for the organization's business are encrypted.
- Only encrypted devices should be used to access Vetiva portal or storage

- Data Transmission

Sensitive data or information must be encrypted before transmission. Data transmissions should be conducted using a Secure Socket Layer (SSL) or an equivalent encryption protocol pre-approved by IT.

- File Encryption

In instances where a whole device cannot be encrypted, measures should be taken to ensure individual files are encrypted before transit or storage. Files encrypted must meet the barest minimum standard for encryption.

- Encryption Standard

All encryption technology must meet a minimal standard.

Technology used to encrypt devices that exceed the standard are permitted to be used while Devices or transmissions that fail to meet the standard may not be employed to store or transmit sensitive data.

- Encryption Key Management

Keys used for encryption shall be stored separately and must not be shared in sight or publicly.

11. Data Disclosure

Vetiva shall ensure that personal data is not disclosed to unauthorised third parties. All Employees/Staff shall exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of Vetiva's business.

All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Officer.

12. Data Retention and Disposal

Vetiva complies with GDPR/NDPA and other relevant local laws, standards and guidelines regulating the retention and destruction of personal data, documents and information. As such, Vetiva shall not keep personal data in a form that can identify data subjects for a longer than is necessary, in relation to the purpose(s) for which the data was originally collected.

The retention period for each category of personal data is set at 6 years in the Vetiva Retention of Records policy along with the criteria used to determine this period including any statutory obligations Vetiva has to retain the data.

Personal data must be disposed of securely in accordance with the principle of the GDPR/NDPA – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects. Any disposal of data will be done in accordance with the Secure Disposal Procedure.

13. Data Transfer

Vetiva will adopt approved Model Contract Clause (MCC) for the transfer of data to foreign countries.

In the absence of an adequacy decision, Model Contract Clauses, a transfer of personal data to a foreign or international organisation shall only take place on one of the following conditions:

i. the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
ii. the transfer is necessary for the performance of a contract between the data subject and Vetiva or the implementation of pre-contractual measures taken at the data subject's request;
iii. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
iv. the transfer is necessary for important reasons of public interest;
v. the transfer is necessary for the establishment, exercise or defence of legal claims; and/or
vi. the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.