



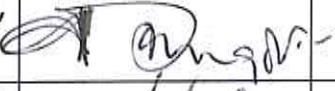

**DANGOTE
INDUSTRIES
LIMITED**

DATA PROTECTION POLICY

Revision History

Version	Date	Revision
1.0		Initial Version

This Data Protection Policy has been reviewed and approved by the Board:

NAME	DESIGNATION	SIGNATURE	DATE
Aliko Dangote	President/Chief Executive, Dangote Industries Limited		
Olakunle Alake	Group Managing Director, Dangote Industries Limited		

Contents

Contents3

1	Introduction	5
1.1	Scope	5
1.2	Document classification and ownership	5
1.3	Document maintenance	5
1.4	Applicable Data Protection Regulations.....	5
2	Definitions.....	5
3	Data Protection Governance	7
3.1	Data Protection Governance	7
3.2	Data Protection Officer	7
4	Processing of Personal Data	8
4.1	Lawful Processing	8
4.2	Procuring Consent	8
4.3	Data Privacy Policy.....	9
4.4	Security and Confidentiality.....	9
4.5	Protecting the Rights of Data Subject.....	9
4.6	Sensitive Personal Data	10
4.7	Processing Personal Data for Marketing Purposes	11
4.8	Transfer of Personal Data.....	11
	4.8.1 Third Party Transfers	11
	4.8.2 Foreign Transfer	11
	4.8.3 Inter-Company transfers	12
5	Data Protection Measures.....	13
5.1	Technical and Organizational Measures	13
	5.1.1 Encryption.....	13
	5.1.2 Physical Access Control	13
	5.1.3 Logical Access Control.....	13
	5.1.4 Data Retention Policy.....	13
	5.1.5 Incident Management	13
	5.1.6 Human Resource Security	13
	5.1.7 Endpoint Protection	13
	5.1.8 Backup and Recovery	14
	5.1.9 Network Security	14
	5.1.10 Security of Non-Electronic Media	14
6	Data Protection Impact Assessment (DPIA).....	15
7	Personal Data Breach.....	16
7.1	Reporting a Personal Data Breach.....	16
8	Data Privacy Audits.....	17
9	Compliance	18

10	Training and Awareness	19
11	Contact	20
	Appendix I.....	21

1 Introduction

This Policy documents Dangote Industry Limited's (DIL) commitment in ensuring protection of Personal Data in line with the requirements of applicable data protection regulations.

1.1 Scope

This Policy has been developed for DIL and is applicable to the processing of Personal Data by DIL and third parties who process Personal Data on behalf of DIL.

1.2 Document classification and ownership

This Policy is owned by the Group Chief Legal Officer.

1.3 Document maintenance

This Policy will be reviewed at least on an annual basis or following any change in the data protection regulation.

1.4 Applicable Data Protection Regulations

This Policy has been designed to enable compliance with relevant data protection regulations such as

- The Nigeria Data Protection Regulation 2019.
- Other applicable global standards and regulations on data privacy

2 Definitions

- "Data Subject" means any person, who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
- "Personal Identifiable Information (PII)" means information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in a context.
- "Personal Data" means any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifiers such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM, Personal Identifiable Information (PII) and others.
- "Sensitive Personal Data" means data relating to religious or other beliefs, sexual orientation, health, race, ethnicity, political views, trades union membership, criminal

records or any other sensitive personal information.

- "Consent" of the Data Subject means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, through a statement or a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her.
- "Data Controller" means a natural or legal person who either alone, jointly with other persons or in common with other persons or a statutory body determines the purposes for and the manner in which Personal Data is processed or is to be processed. In the context of this Policy, "Data Controller" refers to DIL.
- "Data Processor" or "Third Party" means a natural or legal person, which processes Personal Data on behalf of the Data Controller.
- "Processing" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, 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" means the assessment of the impact of a processing operation on the protection of Personal Data (hereafter "DPIA").
- "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.
- "Process Owner" means the person within a department who is responsible for driving compliance with applicable data protection regulation and standards. It will be, in principle, the Head of the Department.
- "Relevant Authorities" means The National Information Technology Development Agency (NITDA) or any other statutory body or establishment having the Government mandate to deal solely or partly with matters relating to Personal Data.
- "Data Protection Compliance Organization (DPCO)" means any entity duly licensed by NITDA for the purpose of training, auditing, consulting and rendering services and products for the purpose of compliance with this Regulation or any foreign Data Protection Law or Regulation having effect in Nigeria.
- "Inter-Company Transfer" refers to the transfer of data between DIL and other entities within the Dangote Group.

3 Data Protection Governance

3.1 Data Protection Governance

In order to enforce compliance with this Data Protection Policy, a Data Protection Governance structure shall be in place at DIL at all times.

3.2 Data Protection Officer

DIL shall designate a Data Protection Officer ("DPO") within the Compliance function who shall report to the Group Chief Legal Officer.

The DPO's tasks shall consist of the following:

- Continuously assess DIL's compliance with applicable Data Protection Laws through performance of audits and periodic spot checks
- Provide recommendations and drive implementation of data protection standards to achieve compliance with internal policies and regulatory requirements
- Drive the delivery of appropriate data privacy training and capacity building programs for all DIL personnel
- Serve as the primary point of contact for Relevant Authorities and DPCO
- Develop a data asset inventory and continuously ensure that the inventory is up-to-date
- Develop a methodology for performing Data Protection Impact Assessment (DPIA) and conduct such assessments on a regular basis
- Assess all instances of personal data breach and notify Relevant Authorities and Data Subjects as required
- Perform due diligence over prospective Third Parties who may process Personal Data on behalf of DIL to ascertain that the parties do not have records of violating the rights of Data Subjects

4 Processing of Personal Data

DIL Personnel or any third party acting on its behalf shall comply with the following principles when processing Personal Data.

4.1 Lawful Processing

DIL Personnel shall ensure that Processing is based on at least one of the following six legal basis:

- 4.1.1 Consent: the Individual has given their explicit consent to the processing of their Personal Data for one or more specific purposes. In addition,
- DIL shall be able to demonstrate that the Individual has consented to processing of their Personal Data, and
 - Prior to giving consent, the Individual shall be informed of their right to withdraw their consent at any time. At consent's withdrawal – which must be as easy as giving consent – the processing must cease.
- 4.1.2 Contract: processing is necessary for:
- the performance of a contract to which the Data Subject is party; or
 - entering into a contract at the request of the Data Subject only.
- 4.1.3 Legal obligation: processing is necessary for compliance with a legal obligation to which DIL is subject;
- 4.1.4 Vital interest: processing is necessary in order to protect the vital interests of the Individual or of another natural person;
- 4.1.5 Public interest: processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in DIL
- 4.1.6 Proper Motives: DIL shall not seek consent that may engender direct or indirect propagation of atrocities, hate, child rights violation, criminal acts and anti-social conducts;

4.2 Procuring Consent

The following guiding principles are applicable for procuring consent from Data Subjects for the purpose of obtaining and processing their Personal Data in line with section 4.1.1 of this Policy:

- DIL will only collect Personal Data after disclosing the purpose of collection to the data subject. Furthermore, DIL will not process Personal Data in a manner that is incompatible with the originally stated purposes.
- DIL will only obtain consent from Data Subjects who have the legal capacity to do so.
- DIL will only obtain consent in a manner that is without fraud, coercion or undue influence. The request for consent shall be presented in an intelligible and easily accessible form, using clear and plain language.
- DIL should be able to demonstrate to the Relevant Authorities at all times that consent has been obtained from Data Subjects for the processing of their personal data
- DIL shall obtain consent where Personal Data may be transferred to a third party.

- DIL shall obtain consent where Personal Data will be transferred to a foreign country with inadequate Data Protection Legislation.

4.3 Data Privacy Policy

For every Personal Data collected, a Privacy Policy specific to the data being collected shall be documented in a written form and displayed on the medium through which the data is obtained. The Privacy Policy shall be simple, conspicuous and easily understood by the class of data subject targeted. Furthermore, the Data Subject will be required to read and provide verifiable consent to DIL for obtaining and processing their Personal Data.

These mediums include the following:

- Electronic forms (including web forms, electronic documents)
- Emails
- Paper-based forms
- Web tokens
- Cookies

The Privacy Policy shall address the following:

- Specification of personal data being collected where this has not been explicitly defined in the medium being used (e.g. through named fields in forms)
- Purpose of collection of Personal Data and legal basis for processing
- Methods used to collect, store and process the personal data
- Access by third parties and the purpose of such access
- Transfer of Personal Data to a foreign country
- The Rights of Data Subjects
- DIL's commitment to ensuring protection of the Personal Data
- Remediation measures in the event the Privacy Policy is violated and timeframe for remediation

4.4 Security and Confidentiality

DIL will take reasonable precautions to secure Personal Data against accidental or unlawful destruction or loss, alteration, unauthorized disclosure or access. These precautions include technical, physical and organizational security measures to prevent unauthorized access, as documented in Section 5 of this Policy. In order to manage proliferation of Personal Data and security concerns associated with such proliferation, DIL should minimize duplication of data collection activities. Effective data governance and management processes should be in place to enable subsequent referencing and processing of existing personal data assets rather than requesting for such information from Data Subjects multiple times. However, all subsequent processing activities personal data must meet the requirements of lawful processing as defined in Section 4.1 of this Policy.

4.5 Protecting the Rights of Data Subject

Individuals have rights when it comes to our handling of their Personal Data. Those rights include:

- The right to request for access to their Personal Data where those requests are reasonable and permitted by law or regulation. DIL shall provide reasonable and accessible means for Individuals to submit their requests, which do not have to take any specific form and can be submitted by any method. DIL shall take appropriate measures to provide the requested information in writing, through electronic means or orally, in line with request of the Data Subject, provided that the identity of the Data Subject has been verified. DIL shall provide such information free of charge, except where it has been demonstrated that the requests are unfounded and excessive. In the event of unfounded and excessive request by the Data Subjects, DIL may either charge a reasonable fee for the administrative costs or write a letter to the Data Subject stating refusal act on the request and copy the Relevant Authorities on every such occasion. Where DIL has reasonable doubts concerning individual making the request, DIL may request the provision of additional information necessary to confirm the identity of the Data Subject. Within 30 days of validating the identity of any Individual submitting a request for access to their Personal Data, DIL shall provide the requested information, or provide legitimate reasons for not complying with their request.
- The right to request that DIL erase their Personal Data if it is no longer valid or necessary for the purposes for which it was collected or if it is incomplete or inaccurate. DIL shall delete such Personal Data based on request from the Data Subject and shall take reasonable steps to notify all Third Parties to delete such Personal Data.
- The right to rectify or amend inaccurate or incomplete Personal Data.
- The right to withdraw their Consent at any time.
- The right to object to DIL's processing of their Personal Data if there are compelling legitimate grounds to do so and to the extent permitted by law or regulation. Individuals have the right to object to DIL's processing of their Personal Data for direct marketing purposes.
- The right to obtain restriction of DIL's processing of their Personal Data if one of the following applies: (i) the accuracy of the Personal Data is contested, (ii) the processing is unlawful, (iii) the Controller no longer needs the Personal Data for the purposes of processing, and (iv) the Individual has objected to the processing as set out above.
- The right to receive their Personal Data in a commonly used and machine-readable format and the right to transmit these data to another Data Controller when the processing is based on (explicit) consent or when the processing is necessary for the performance of a contract.

4.6 Sensitive Personal Data

DIL Personnel shall not process Sensitive Personal Data unless one of the following legal bases is met:

- The Individual gave explicit consent to the data processing;
- Processing is carried out by a non-profit body with political, philosophical, religious or trade union purposes in the course of its legitimate activities and only relates to its (former) members or to persons who have regular contact with it for such purposes;
- Processing concerns data explicitly made public by the Individual;
- Processing is necessary:

- to carry out the obligations of, and to exercise the specific rights of, DIL or of the Individual in the employment
- to protect the vital interests of the Individual or another natural person (when the Individual cannot give consent);
- to establish, exercise or defend legal claims or when courts act in their judicial capacity;
- for preventative or occupational medicinal purposes: "for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services law or pursuant to contract with a health professional";
- for public interest reasons in the area of public health; or
- for substantial public interest reasons.

Note: to process special categories of data, a contractual relationship with the data subject is thus not viewed as a legal basis for the legitimate processing of sensitive data, except for a contract with a health professional subject to the obligation of professional secrecy

4.7 Processing Personal Data for Marketing Purposes

DIL Personnel will not process Personal Data for the purposes of direct marketing, unless the individual provided valid consent and effective procedures are implemented allowing Individuals to withdraw their consent at any time.

4.8 Transfer of Personal Data

DIL shall transfer and store Personal Data to entities within the Dangote affiliates and subsidiaries and third parties on our behalf within and outside Nigeria for legitimate business activities in accordance with Data Protection Laws and professional standards.

4.8.1 Third Party Transfers

DIL will ensure that any transfer of Personal Data to a third party is governed by written agreements with third parties that impose obligations that reflect the requirements of Data Protection Regulations and this Policy. Such contracts should include non-disclosure agreements (NDAs) and indemnity clauses which would ensure DIL is indemnified of any losses or penalties arising from a breach of the Data Protection Regulations by such third parties.

4.8.2 Foreign Transfer

DIL shall not transfer Personal Data to another country or organization outside Nigeria unless the Company is satisfied that the Personal Data is adequately protected in accordance with Data Protection Laws. DIL shall rely on the decision of the Relevant Authorities and the Honorable Attorney General of the Federation (HAGF) in determining which countries or foreign jurisdictions have implemented adequate safeguards for the protection of Personal Data. Where there is no decision by the Relevant Authorities or HAGF, DIL may transfer Personal Data to a foreign country, provided any of the following conditions are met:

- that the Data Subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers;
- the transfer is necessary for the performance of a contract between the Data Subject and the Controller or the implementation of pre-contractual measures taken at the Data Subject's request;
- 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;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; and
- 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; provided, in all circumstances, that the Data Subject has been manifestly made to understand through clear warnings of the specific principle(s) of data protection that are likely to be violated in the event of transfer to a third country, this proviso shall not apply to any instance where the Data Subject is answerable in duly established legal action for any civil or criminal claim in a third country.

4.8.3 Inter-Company transfers

Transfers of Personal Data to other entities within Dangote affiliates and subsidiaries will be subject to the terms of this Policy. This also includes the storage or processing of Personal Data on information systems that can be accessed by other Dangote affiliates and subsidiaries. All Dangote affiliates and subsidiaries should be signatories to an inter-company agreement that includes contractual terms to ensure the protection of the Personal Data being transferred in accordance with the terms of this Policy.

5 Data Protection Measures

DIL shall implement appropriate measures to ensure and to be able to demonstrate that the processing of Personal Data is performed in accordance with Data Protection Laws, taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of the Individuals.

5.1 Technical and Organizational Measures

The following technical and organizational measures will be in place:

5.1.1 Encryption

Implement encryption techniques on all categories of electronic Personal Data including data at rest and data in transit in order to restrict ability to comprehend such data to authorized personnel only.

5.1.2 Physical Access Control

Ensure that all infrastructure and facilities housing Personal Data both in electronic and non-electronic formats are protected with adequate physical access controls in order to minimize the risk of unauthorized access.

5.1.3 Logical Access Control

Implement logical access controls including configuration of access rules, identification and strong authentication mechanisms over information systems hosting Personal Data in order to restrict access to authorized individuals only.

5.1.4 Data Retention Policy

Develop and implement a data retention policy, which would ensure that Personal Data is not retained for longer than necessary in order to reduce the likelihood and/or severity of a data breach.

5.1.5 Incident Management

Implement an effective process, which ensures adequate detection and response to incidents and security breaches that may expose Personal Data.

5.1.6 Human Resource Security

Implement measures to reduce the risk of DIL personnel breaching data protection regulations. These measures will be in place prior to staff employment (e.g. through adequate background checks), during employment (e.g. through effective end user information security awareness programs) and post-employment (through appropriate deactivation process).

5.1.7 Endpoint Protection

Implement an endpoint protection solution on all workstations and servers, including anti-malware solutions, in order to minimize the possibility of a breach in protection of Personal Data.

5.1.8 Backup and Recovery

Perform regular backups of data stored in servers and workstations to ensure availability of Personal Data in line with backup policies.

5.1.9 Network Security

Minimize the risk of breach to Personal Data through network and connectivity channels. This is achieved through adequate, network segmentation, firewall, network access control, intrusion prevention and detection, SSH protocol, strong authentication, etc.

5.1.10 Security of Non-Electronic Media

Reduce the risks of unauthorized access to physical documents containing Personal Data through appropriate document classification, securing printing equipment, clear desk policies, amongst other measures. Print security can be enhanced through appropriate authentication methods and secure release of printouts as well as chargeback and accounting measures, which can minimize proliferation of physical printouts.

6 Data Protection Impact Assessment (DPIA)

DIL shall perform DPIAs every two years or earlier in the cases of a significant change to the business or technology environment in order to identify, analyse and mitigate the risks associated with processing Personal Data. These risks include unlawful processing as well as any compromise of the confidentiality, integrity and accuracy of such data.

In addition to the DPIAs, an assessment would be necessary prior to any the following events:

- The introduction of a new processing technology
- Significant changes to business processes and technology solutions that have touchpoints with Personal Data
- Where DIL intends to collect a new type of Personal Data in order to perform business operations
- Whenever the Relevant Authorities communicate issues a list of processing operations for which a DPIA is required.
- Where Personal Data will be transferred to a Third Party or a foreign country

The Assessment shall cover the following:

- A description of the envisaged processing operations and the purposes of the processing
- An assessment of the necessity and proportionality of the processing operations in relation to the purposes
- An assessment of the risks to the rights and freedoms of data subjects
- Description of measures to mitigate the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data and to demonstrate compliance with this Regulation.

DIL shall consult the Relevant Authority before starting the processing operation, if it appears that the processing will result in a high risk for the rights of individuals and no effective measures are in place to mitigate the risk.

7 Personal Data Breach

7.1 Reporting a Personal Data Breach

All DIL Personnel who suspect or become aware of a Data Breach will immediately report it to the Group Chief Legal Officer and if the Data relates to information on Computers or electronic device or system to the Chief Technology Officer.

Where Personal Data is involved, DIL Personnel should immediately report it through dpo.dil@dangote.com

DIL Personnel will not attempt to investigate any suspected/proven breach themselves, nor discuss the case with any third parties, unless they are instructed or authorized to do so by the Legal Department.

DIL shall maintain a Personal Data Breach Register. Any Personal Data Breach will be recorded in the Personal Data Breach Register.

The DPO has a duty of Self-Reporting Data Breaches to NITDA within 72 hours of his/her knowledge of the breach. The Report should include the amount of data likely to be affected, cause of breach and remedial actions being taken.

8 Data Privacy Audits

DIL shall engage the services of a Data Protection Compliance Organization (DPCO) on an annual basis to perform an audit of its data privacy and protection practices. The primary objective of this audit is to assess compliance to the Nigeria Data Protection Regulation and provide attestation of such compliance to the Relevant Authorities and other stakeholders.

The Data Privacy and Protection Audit report would state the following:

- personally identifiable information that DIL collects on employees of the organization and members of the public
- any purpose for which the personally identifiable information is collected
- any notice given to individuals regarding the collection and use of personal information relating to that individual
- any access given to individuals to review, amend, correct, supplement, or delete personal information relating to that individual
- whether or not consent is obtained from an individual before personally identifiable information is collected, used, transferred, or disclosed and any method used to obtain consent
- the policies and practices of the organization for the security of personally identifiable information
- the policies and practices of the organization for the proper use of personally identifiable information
- the policies and procedures of the organization for privacy and data protection
- the policies and procedures of the organization for monitoring and reporting violations of privacy and data protection policies
- the policies and procedures of the organization for assessing the impact of technologies on the stated privacy and security policies.

The DPO will serve as the primary liaison with the DPCO for the purpose of the audit and will drive the remediation of any exceptions identified from the audit in order to achieve full compliance with regulatory requirements.

9 Compliance

Non-compliance with Data Protection Laws may have serious consequences on the impacted individuals. As a result, compliance with this Policy is mandatory. DIL Personnel found to be in breach of this policy shall be subject to a disciplinary process, which may include dismissal. DIL personnel will be required to provide a declaration of compliance to the Data Protection Policy on an annual basis.

Note: non-compliance may result in potential fines for DIL of up to 10 million Naira or 2% of global annual turnover depending on the nature of the breach. In addition, breaches of Data Protection Laws can give rise to criminal and/or civil liability.

10 Training and Awareness

DIL shall conduct mandatory annual data protection training and periodic privacy awareness communications to DIL Personnel who may collect, access and or process personal data. Records of training attendance will be maintained and monitored. This training program will include an assessment test to evaluate understanding of the Data Protection Policy. Non-completion of this mandatory training and assessment test within the defined timelines will amount to a breach of this Policy.

11 Contact

Any question regarding this policy can be addressed to the DPO at dpo.dil@dangote.com

Appendix I

The table below documents DIL's Personal Data assets and their relevant attributes. This list will be updated on a regular basis as Data Privacy Impact Assessments are conducted.

A Data Privacy Policy shall be developed for every data asset in this list in line with Section 4.3 of this Policy

Process Owner	Data Asset	Personal Identifiable Information	Purpose for Collection	Collection Medium	Storage Location
Credit Risk Department	Customer Data	<ul style="list-style-type: none"> Name Phone Number Date of Birth Email Address Residential address Gender Nationality Marital Status National ID Number Passport Number Driver's License Number Bank Verification Number (BVN) Name of Guarantor Relationship with the Beneficiary Address of Guarantor 	Know your Customer (KYC)	Paper-based Forms (Customer Application form)	<ul style="list-style-type: none"> SAP Servers File cabinets of Sales & Credit Departments respectively (Ikoyi, Lagos)
Procurement	Vendor Data	<ul style="list-style-type: none"> Contact Information: Name of Contact Person, Email Address, Phone Number Bank details: Account number, Bank name, Account Holder 	Vendor registration	Paper-based Forms (vendor registration form)	<ul style="list-style-type: none"> SAP Servers
Human Resources	Employee Data	<ul style="list-style-type: none"> Name Phone number Date of Birth Email address Employment start date Place of birth Country of birth State of origin State of residence Nationality 	<ul style="list-style-type: none"> Recruitment processing Human Capital Management 	<ul style="list-style-type: none"> Paper-based forms (Physical recruitment forms) Web Forms (Recruitment portal) Email (including electronic attachments) 	<ul style="list-style-type: none"> SAP Servers File cabinets of HR Departments respectively (Ikoyi, Lagos) User workstations

		<ul style="list-style-type: none"> • Marital status • Name of spouse • Religion • Personal phone number • Official phone number • Residential address • Academic History • Banking Details • Next of kin information • Beneficiary Information • Emergency Contact 			
Human Resources	Reference Data	<ul style="list-style-type: none"> • Referee's Name • Place of Work • Email • Relationship • Telephone • Previous Employer • Name of Organisation • Date of Employment • Date of Leaving • Entry Position • Entry Compensation • Course • Academic History 	Recruitment processing; verification of employment and academic history	<ul style="list-style-type: none"> • Paper-based forms (Physical recruitment forms) • Web Forms (Recruitment portal) • Email (including electronic attachments) 	<ul style="list-style-type: none"> • SAP Servers • File cabinets of HR Departments respectively (Ikoyi, Lagos) • User workstations
Human Resources	Beneficiary Information	<ul style="list-style-type: none"> • Number of beneficiary • Relationship • Percentage allotted • Bank account details • Address • Phone Number 	Processing of employee benefit plan	<ul style="list-style-type: none"> • Paper-based forms (Physical recruitment forms) • Web Forms (Recruitment portal) • Email (including electronic attachments) 	<ul style="list-style-type: none"> • SAP Servers • File cabinets of HR Departments respectively (Ikoyi, Lagos) • User workstations