DANGOTE CEMENT

DATA PROTECTION POLICY

Policy History

Version	Year/Approval	Remark
1.0	January 2025	First version

This Policy has been approved by the Board:

S/N	Name	Designation	Signature
1.0	Arvind Pathak	Group Managing Director	
2.0	Ernest Ebi, MFR	Chairman, Board Audit, Compliance & Risk Management Committee	
3.0	Emmanuel Ikazoboh	Chairman, Remuneration, Governance and Nominations Committee	
4.0	Aliko Dangote, GCON	Chairman, Board of Directors	

Prepared by: Legal Department

TABLE OF CONTENT

1.0 Introduction:

Dangote Cement PLC (the "Company" or "Dangote") which expression shall include all its subsidiaries, is committed to protecting the privacy and security of personal and sensitive information, while respecting individual privacy rights.

This Data Protection Policy outlines principles and practices to ensure compliance with applicable data protection laws.

2.0 Scope:

The Policy applies to all personal data collected, processed, or stored by the Company, including data from employees, customers, business partners, vendors, service providers, suppliers, and agents.

3.0 Applicable Data Protection Regulations & Laws:

3.1 The Policy complies with relevant data protection regulations and laws, including:

i. The Constitution of the Federal Republic of Nigeria 1999.

ii. The Freedom of Information Act 2011.

iii. Cybercrimes (Prohibition, Prevention, etc.) Act 2015.

iv. Nigeria Data Protection Regulation 2019 (NDPR).

v. NDPR Implementation Framework 2020.

vi. Nigeria Data Protection Act 2023.

4.0 Definitions:

4.1 **Data Subject:** Data Subjects are natural persons whose personal data is being processed by a Data Controller or Data Processor.

4.2 **Personal Identifiable Information (PII):** Personal Identifiable Information (PII) is information used to identify, contact, or locate a person or individual in a context.

4.3 **Personal Data:** Personal Data refers to information relating to an identifiable natural person, such as name, identification number, location data, or factors specific to their physical, physiological, genetic, mental, economic, cultural, or social identity. It can include names, addresses, photos, bank details, and medical information.

4.4 **Sensitive Personal Data:** Sensitive personal data includes religious beliefs, sexual orientation, health, race, ethnicity, political views, trade union membership, and criminal records.

4.5 **Consent of the Data Subject:** Consent from the Data Subject is a voluntary, specific, and informed agreement to the processing of their Personal Data.

4.6 **Processing:** Processing involves any operation or set of operations on any Data, including collection, organization, storage, and disclosure.

4.7 **Data Protection Impact Assessment:** Data Protection Impact Assessment assesses processing operations' impact on Personal Data protection.

4.8 **Personal Data Breach:** Personal Data Breach refers to security breaches resulting in accidental or unlawful destruction, loss, alteration, or unauthorized disclosure.

4.9 **Process Owners:** Process Owners are department heads responsible for data protection compliance.

4.10 **Relevant Authorities:** Relevant Authorities, such as the Nigeria Data Protection Commission, are statutory bodies mandated by the government to handle Personal Data matters.

4.11 **Data Protection Compliance Organization (DPCO):** The Nigeria Data Protection Bureau license entities (DPCOs) for training, auditing, consulting, and providing services in compliance with NDPR or foreign data protection laws.

4.12 **Data Controller:** A Data Controller, whether an individual, company, or public authority, is responsible for processing personal data, obtaining consent, ensuring data quality, providing notice, implementing security measures, and respecting data subjects' rights.

4.13 **Data Processor:** Under NDPA 2023, a Data Processor is a person or company responsible for handling Personal Data on behalf of a Data Controller. They handle organizing, transferring, processing, verifying, updating, and reporting data. Data Processors, like HMOs and banks, must follow Data Controllers' instructions and protect data.

4.14 **Inter Company Transfer:** Inter-company transfers involve data transfers between entities within a Company.

4.15 **Employee (s):** Employees refer to all permanent, contract, or temporary employees of the Company.

4.16 **Employee Data:** Employee data includes personal details, contact information, employment history, and performance records.

4.17 **Data Retention:** Data retention is determined by the Company's policies and legal requirements.

4.18 **Data Erasure** (Right to be Forgotten): Data subjects have the right to request deletion when necessary or withdraw consent.

4.19 **Data Portability:** Data Portability allows data subjects to transfer their data to another controller.

4.20 **Privacy Impact Assessment (PIA):** Privacy Impact Assessment assesses potential privacy risks.

4.21 **Nigeria Data Protection Regulation 2019 (NDPR):** The Nigeria Data Protection Regulation 2019 (NDPR) is Nigeria's first comprehensive data protection regulation.

4.22 **Nigeria Data Protection Act 2023:** The Act establishes the legal framework for regulating personal data in Nigeria, and replaces the Nigerian Data Protection Regulations (NDPR) 2019 and the NDPR Implementation Framework 2019, which were previously issued under the National Information Technology Development Agency (NITDA) Act.

4.23 **Nigeria Data Protection Commission:** The Nigeria Data Protection Commission (NDPC) is an independent authority established by the NDPA to enforce and implement the Act, issuing regulations, conducting investigations, and imposing penalties for violations.

4.24 **Data Rectification:** Data rectification is a free process for correcting inaccurate or deficient data, with the Data Controller having the right to charge a reasonable fee or refuse the request.

5.0 Data Protection Governing Principles:

5.1 The Company upholds data protection principles such as lawfulness, fairness, transparency, purpose limitation, data minimization, and accuracy.

5.2 The Company processes Personal Data lawfully, fairly, and in a transparent format, ensuring it is relevant, adequate, and up to date for its intended purposes.

5.3 The Company ensures data retention for its intended purpose, maintains security and confidentiality, and is accountable for its compliance with these principles, ensuring data protection against unauthorized access, disclosure, alteration, and destruction.

6.0 Data Protection Responsibilities:

6.1 The Nigeria Data Protection Act 2023 mandates data protection responsibilities for Data Controllers and Processors in Nigeria, including compliance with data collection, storage, use, and sharing duties.

6.2 The Act outlines the process of collecting and processing personal data, obtaining consent, providing access, rectifying, or deleting data, securing it against unauthorized access, notifying the Commission of data breaches, conducting data protection impact assessments, appointing a Data Protection Officer, registering with the Commission, paying fees, and adhering to data protection principles.

6.3 The NDPA imposes penalties for non-compliance with data protection responsibilities, highlighting the need for Data Controllers and Processors to be aware of their obligations.

7.0 Data Protection Officer (DPO): Each subsidiary must designate a Data Protection Officer (DPO) to report to the General Counsel/Company Secretary, as mandated by NDPR 2019 and NDPA 2023.

7.1 **The DPO is responsible for:**

- 7.1.1 assessing the Company's compliance with Data Protection laws.
- 7.1.2 providing recommendations.
- 7.1.3 implementing data protection standards.
- 7.1.4 delivering data privacy training.
- 7.1.5 serving as the primary point of contact for authorities and DPCOs.
- 7.1.6 developing a Personal Data asset list.
- 7.1.7 conducting regular Data Protection Impact Assessments.
- 7.1.8 evaluating all instances of Personal Data breaches and informing the appropriate authorities and Data Subjects as needed.
- 7.1.9 conducting due diligence on potential third parties processing Personal Data, ensuring they do not have any records of data subject rights violations.

Note: For data protection enquiries, Employees are advised to send an email to dpo.dcp@dangote.com or contact the Legal Department, DCP.

8.3 Objectives of the NDPA:

The NDPA aims to:

- 8.3.1 regulate and promote data processing.
- 8.3.2 ensure security and privacy.
- 8.3.3 protect data subjects' rights.
- 8.3.4 provide remedies for data breaches.
- 8.3.5 ensure data controllers and processors fulfil their obligations.
- 8.3.6 establish the Nigeria Data Protection Commission.
- 8.3.7 maintain international trade competitiveness and create sustainable jobs.

8.4 Application of the NDPA:

8.4.1 The NDPA applies to all processing of Personal Data within Nigeria, where the Data Controller or Processor is a Nigerian resident, operates in Nigeria, or is domiciled in Nigeria.

8.5 Exemptions of the NDPA:

8.5.1 The Nigeria Data Protection Act (NDPA) has exemptions for processing personal data in certain situations, such as:
8.5.1.1 personal or household purposes.
8.5.1.2 lawful crime prevention.
8.5.1.3 national public health emergencies.
8.5.1.4 national security.
8.5.1.5 public interest publication, and
8.5.1.6 legal claims defence.

8.6 Key Highlights of the NDPA:

The key highlights of the NDPA are listed below:

8.6.1 The NDPA applies to natural persons residing or operating in Nigeria, Data Processors or Controllers, and all transactions for the processing of Personal Data within Nigeria.

8.6.2 The Act outlines strict compliance obligations for Data Controllers and Data Processors.

8.6.3 The appointment of a Data Protection Officer (DPO), is mandatory for Data Controllers or Processors of significant importance.

8.6.4 Data Protection Impact Assessment (DPIA): This is a crucial process for assessing the rights of data subjects in new projects or activities.

8.6.5 Consent must be freely given by the Data Subject, it cannot be obtained through fraud, coercion, or undue influence, and the Data Subject has the right to withdraw it.

8.6.6 Data Subjects' rights and individual rights are closely related but not the same:

8.6.6.1 Data Subjects' rights are specific rights granted to individuals whose personal data is being processed. See clause 9.5 below.

8.6.6.2 Individual rights are broader rights that apply to all individuals, not just Data Subjects. Individual rights encompass various aspects of privacy, freedom, and protection.

8.6.7 Severe penalties include a maximum fine of 2% of annual revenue or N10 million for major Data Controllers or Processors, administrative sanctions by the NDPC, and criminal prosecution.

8.6.8 The principles governing data processing include unlawful processing, purpose limitation, data minimization, retention limit, accuracy, security, confidentiality, integrity, and accountability.

8.6.9. The legal basis for processing personal data includes consent, contractual obligations, legal obligations, vital interest, public interest, official mandate exercise, and legitimate interest.

8.6.10 The Data Controller must ensure Data Subjects understand its privacy policy, appoint a Data Protection Officer, provide necessary information, and inform them about the reasons for data processing.

8.6.11 The NDPA and the NDPC are responsible for managing the transfer of personal data to foreign countries, ensuring adequate protection.

9.0 Processing Personal Data:

9.1 The NDPA mandates that the Company's personnel or a third party acting on its behalf, must adhere to specific principles when processing personal data, ensuring it is processed legally.

9.1.1 Consent: The Data Subject must give their consent for their personal data to be processed, and the Company must prove this. The Data Subject has the right to withdraw consent, which must be easy.

9.1.2 Contract: The processing of Personal Data is necessary for the fulfillment of a contract the Data Subject is a party to and for entering into a contract at their request.

9.1.3 Legal Obligation: The Company is subject to legal obligations when the processing of Personal Data is necessary for compliance.

9.1.4 Vital Interest: Personal Data processing is necessary to safeguard the vital interests of the Data Subject or another natural person.

9.1.5 Public Interest: Personal Data processing is necessary for public tasks or exercising official authority vested in the Company, as it is necessary for the performance of these tasks.

9.1.6 Proper Motives: The Company is prohibited from obtaining consent that could potentially lead to the spread of atrocities, hate, child rights violations, criminal acts, and anti-social behavior.

9.2 Procuring Consent:
As outlined in Section 9.1.1 of this Policy other procedures for obtaining consent from Data Subjects for the collection and processing of their personal data, are itemized below:

9.2.1 The Company will only collect Personal Data after disclosing its purpose to the Data Subject and will not process it in a way that contradicts its original purpose.

9.2.2 In line with the provision of the NDPA, where a data subject is a child or a person lacking the legal capacity to consent, a data controller shall obtain the consent of the parent or legal guardian. Some exceptions however include protecting minors' interests, providing confidentiality services, or for court proceedings. Data Controllers must verify age and consent through government-approved identification documents.

9.2.3 Where the circumstance relates to the processing of personal data of a child of 13 years and above in relation to the provision of information and services by electronic means at the specific request of the child, the Commission shall make regulations in accordance with the objectives of the NDPA.

9.2.4 The Company will ensure consent without fraud, coercion, or undue influence, using clear, plain language in an easily accessible form.

9.2.5 The Company shall always demonstrate to the relevant authorities that consent has been obtained from Data Subjects for the processing of their Personal Data.

9.2.6 The Company is required to obtain consent before transferring Personal Data to a third party.

9.2.7 The Company must obtain consent before transferring Personal Data to a foreign country or jurisdiction with insufficient data protection legislation.

9.3 Data Privacy Policy:
A Privacy Policy for collecting Personal Data must be written, easily understood, and easily accessible to the targeted Data Subject, requiring their verifiable consent for data processing.

9.3.1 Privacy policies can be displayed through various mediums such as electronic forms, emails, paper-based forms, web tokens, and cookies.

9.3.2 The privacy policy should detail the collection, purpose, and processing methods of personal data, as well as the rights of data subjects, the Company's commitment to data protection, and remediation measures in case of policy violations.

9.4. Security and Confidentiality:

9.4.1 The Company will implement security measures to protect Personal Data from accidents, loss, alteration, unauthorized disclosure, and access. It will minimize data duplication and ensure effective data governance for efficient processing. All subsequent processing must meet lawful processing requirements, as outlined in clause 9.1 of this Policy.

9.5 Protecting the Rights of Data Subjects:

Data Subjects have rights regarding the handling of their personal data, which include:

9.5.1 **Right to Request for Personal Data:** The Company must ensure Data Subjects have the right to request access to their Personal Data, provided it is reasonable and permitted by law or regulation.

9.5.1.1 Unless excessive or unfounded, the Company will provide, free of charge, the requested information in written, electronic, or oral form, provided the Data Subject's identity is verified.

9.5.1.2 The Company may charge administrative costs or refuse to act on Data Subjects' requests if they are unfounded or excessive. If the Company has doubts about the Data Subject's identity, additional information may be requested. Within 30 days, the Company must provide information or reasons for not granting the request.

9.5.2 **The right to request for deletion of personal data:** The Company is required to grant the Data Subject's request for the deletion of their Personal Data if it is no longer necessary or incomplete.

9.5.3 The right to rectify or amend inaccurate or incomplete Personal Data: The Act grants Data Subjects the right to rectification of their inaccurate or incomplete Personal Data. They can request rectification verbally or in writing, with a one-month time limit unless complex or multiple requests. The Company can extend the time limit by two months but must inform the Data Subjects of their right to file a complaint or seek judicial remedy.

9.5.4 **The right to withdraw Consent at any time:** The Nigeria Data Protection Act 2023 grants Data Subjects the right to withdraw their consent.

9.5.5 **The right to object to the Company's processing of their Personal Data:** Data subjects have the right to object to the Company's processing of their Personal Data for direct marketing purposes, provided there are compelling and legitimate grounds.

9.5.6 **The right to restrict the Company's processing of Personal Data:** Data Subjects have the right to challenge data processing if the data's accuracy is contested, the process is unlawful, or the Data Controller no longer needs the data.

9.5.7 Data Subjects have the right to receive and transmit their Personal Data in a machine-readable format, either with explicit consent or for the performance of a contract.

9.6 Sensitive Personal Data:

9.6.1 The Company must process Sensitive Personal Data only if the Data Subject gives explicit consent, the processing is done by a non-profit organization, the data is publicly made,

necessary, for employment obligations, protecting vital interests, establishing legal claims, or for preventative or occupational medicinal purposes.

9.6.2 Processing may also be necessary for public health reasons, public interest reasons, or substantial public interest reasons.

Note: Legal basis for processing Sensitive Personal Data is not established by contractual relationships with Data Subjects, except for health professional contracts requiring professional secrecy.

9.7 Processing of Personal Data for Marketing Purposes: The Company will not process Personal Data for direct marketing without valid consent and effective procedures, allowing Data Subjects to withdraw consent at any time.

9.8 Transfer of Personal Data: The Company is required to securely transfer and store Personal Data for legitimate business purposes, in compliance with data protection laws, professional standards, and best practices.

9.8.1 **Third Party Transfers:** The Company will establish written agreements with third parties for data transfer, ensuring obligations align with data protection regulations and policy, including non-disclosure agreements and indemnity clauses.

9.8.2 **Foreign Transfers:** The Company must ensure data protection before transferring it to another country or organization outside Nigeria, relying on authorities and the Attorney General of the Federation for decisions. If no decision is made, the Company can transfer data, but must meet the following conditions:

9.8.2.1 The Data Subject has consented.
9.8.2.2 The transfer is necessary for a contract.
9.8.2.3 Protection of public or vital interests, provided it understands the principles of data protection.

9.8.3 **Inter - Company Transfers:** This Policy governs personal data transfers to affiliates and subsidiaries, including storage and processing on information systems. All affiliates and subsidiaries must sign an inter-company agreement with contractual terms for data protection.

10.0 Data Protection Measures:

The Company is committed to ensuring data processing complies with data protection laws, considering the nature, scope, context, purpose, and risks to Data Subjects' rights and freedoms.

10.1 Technical and Organizational Measures: The Company is committed to implementing the following technical and organizational measures:

10.1.1 **Encryption:** The Company will use encryption techniques to protect electronic Personal Data, converting information into a code to prevent unauthorized access and restrict it to authorized personnel only.

10.1.2 **Physical Access Control:** The Company is committed to protecting all infrastructure and facilities containing Personal Data, both electronic and non-electronic, with robust physical access controls to prevent unauthorized access.

10.1.3 **Logical Access Control:** The Company is committed to implementing logical access controls, including access rules, identification, and strong authentication mechanisms, over information systems hosting Personal Data to restrict access to authorized personnel only.

10.1.4 **Data Retention Policy:** The Company is committed to creating and implementingdata retention processes to minimize the duration of personal data retention and prevent data breaches.

10.1.5 **Incident Management:** The Company is committed to implementing a robust process for swift detection and response to security incidents and breaches that may compromise Personal Data.

10.1.6 **Human Resources Security:** The Company is committed to implementing measures to reduce the risk of personnel breaches of data protection regulations, including background checks, information security awareness programs, and post-employment deactivation processes.

10.1.7 **Endpoint Protection:** The Company is set to implement endpoint protection solutions, including anti-malware solutions, on all workstations and servers to mitigate the risk of Personal Data breaches.

10.1.8 **Backup and Recovery:** The Company is committed to regular data backups on its servers and workstations to ensure the availability of Personal Data in line with backup policies.

10.1.9 **Network Security:** The Company aims to reduce the risk of Personal Data breaches through network segmentation, firewalls, intrusion prevention, secure shell protocol, and strong authentication.

10.1.10 **Security of Non-electronic Media:** The Company aims to minimize unauthorized access to Personal Data-containing physical documents through proper classification, equipment security, and clear policies, enhancing print security.

11.0 Data Protection Impact Assessment (DPIA):

The Company shall conduct DPIAs every two (2) years or earlier to identify, analyze, and mitigate risks related to personal data processing, including unlawful processing, data confidentiality, and integrity compromises.

11.1 An assessment is required for new processing technology, significant changes to business processes, new types of Personal Data collection, authorities' communication of processing operations requiring DPIA, and data transfers to third parties or foreign countries.

11.2 The assessment will detail the purpose, necessity, and proportionality of processing operations, identify risks related to Data Subjects' rights, and outline measures to mitigate these risks, ensuring data protection and compliance with NDPA 2023.

11.3 The Company shall consult with the relevant authority before processing operations if it appears to pose a high risk to Data Subjects' rights without effective mitigation measures.

12.0 Personal Data Breach:

12.1 **Reporting a Personal Data Breach:** The Company requires employees to report any suspected or proven data breach to the Company's General Counsel/Company Secretary, IT/CEO Dancom, Chief Internal Auditor or the Company's Chief Human Resources Officer. They are not allowed to investigate or discuss cases with third parties without permission. The Company maintains a Personal Data Breach Register, and it must self-report breaches to NDPC within 72 hours. Remedial actions are to be taken to prevent recurrence.

13.0 Data Privacy Audits:

The Company will annually hire a Data Protection Compliance Organization (DPCO) to audit its data privacy practices, assessing compliance with the Nigeria Data Protection Regulation 2019 and the Nigeria Data Protection Act 2023.

13.1 The data privacy and audit report outline the organization's collection, use, and disclosure of personal identifiable information on employees and the public. It also details the purpose of collection, notices given to Data Subjects, access to information, and consent obtained.

The report also outlines the Company's policies for security, proper use, privacy, data protection, monitoring, reporting violations, and assessing the impact of technologies on these policies.

Note: The DPO will act as the primary liaison with the DPCO during the audit, ensuring compliance with regulatory requirements by remediating any identified exceptions.

14.0 Monitoring, Compliance and Enforcement:

The Company is committed to enforcing laws and regulations related to employee data privacy, including the Nigeria Data Protection Regulation 2019 and the Nigeria Data Protection Act 2023, and will regularly review and update this Policy.

Note: Non-compliance with data protection laws can lead to fines of up to N10,000,000 (ten Million Naira), or 2% of global annual turnover, criminal and civil liability.

15.0 Data Retention:

The Company's data retention policies aim to comply with legal obligations regarding the retention and deletion of Personal Data. Data processed for customer engagement, recruitment, or employment should be kept for as long as necessary. The Company collects and stores minimal amounts of Personal Data, ensuring relevant third-party data. Documents containing Personal Data will be retained as required by law, relevant to legal proceedings, recruitment, or fraud prevention.

16.0 Training and Awareness:

The Company is committed to educating employees about data privacy, best practices, providing ongoing training and periodic awareness communications. Mandatory annual training and assessment tests will be conducted, with non-compliance resulting in a breach of the Data Protection Policy.

17.0 Employee Data Privacy Consent Clause:

The Company requires all employees to read and understand this Policy and sign the Employee Data Privacy Consent Clause, allowing the Company to process and transfer employee data. If an employee declines consent, the Company may be limited in contractual responsibilities, and will not be liable for employee hardship or loss.

18.0 Policy Review:

This policy may be reviewed every three (3) years or as may be required, to ensure that it remains current and consistent with best practices and applicable laws.

APPENDIX 1 (EMPLOYEE DATA PRIVACY CONSENT FORM)

1. The Company collects, retains, and processes Personal Identifiable Information (PII) for various purposes, including HR management, business management, compliance with laws, protecting the Company's interests, monitoring employees, and conducting audits, compliance checks, and internal investigations. This information is used for recruitment, promotion, training, disciplinary matters, employment references, pay, benefits, services, and dispute resolution processes.

2. The Company may share your personal information with other global companies, service providers, and advisors for the purposes outlined in clause 1.

3. The Company may transfer your Personal Identifiable Information (PII) to third parties during asset reorganization, merger, share purchase, or sale, requiring them to use your PII only for specified transactions.

4. The Company is committed to upholding Nigerian law's requirements for the security of your Personal Identifiable information (PII) transferred abroad.

5. The employee agrees to the Company's management of their personal information and employment terms, including the right to transfer such information to third parties. The information will be used for legitimate business purposes, including human resources management, business management, customer relations, transaction assessment, compliance with laws, audits, and internal investigations.

6. **Data Subject's Rights:** The Company will enable employees to review and update their personal Identifiable information (PII) as per Nigerian data protection laws and regulations.

7. **Consent.** By signing this consent form and returning it to the Company, you agree the collection, retention, and processing of your personal Identifiable Information (PII), including transfers to third parties abroad. Additional consent may be sought if required by law.

8. You can withdraw your consent to this form at any time by providing the Company with written notice.

9. The form is subject to all Nigerian data protection laws and regulations, specifically the Nigeria Data Protection Act 2023.

I, ... hereby consent to the foregoing and confirm that I have received and read the Employee Data Privacy Consent Form.

_____

Signature and Date

APPENDIX 2 (PERSONAL DATA ASSET LIST)

The table outlines the Company's Personal Data assets, updated with DPIAs, and outlines the development of a data privacy policy for each asset.

Process Owner	Data Asset	Personal Identifiable Information	Purpose for collection	Collection Medium	Storage Location
Credit Risk Unit (Risk Department)	Customer Data	Name Phone Number Date of Birth Email address Residential address Gender Nationality Marital status National ID Number Passport Number	Know your Customer (KYC)	Paper-based forms (Customer application form)	SAP servers File cabinets of sales & credit departments respectively (Headquarters).
		Driver's licence Number Bank verification Number (BVN) Name of Guarantor Relationship with the beneficiary Address of guarantor			
Procurement	Vendor Data	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)	SAP servers
Human Resources	Employee Data	Title (Mr/MRS/MISS/MS) Name (Surname, First Name and Middle Name Phone Number Date of birth (DD/MM/YYYY) Email address Employment start date Employment No Place of birth Country of birth State of origin State of residence Nationality National Identity NO Marital status (Single/Married/Widowed/Divorced) If Married, When Name of spouse Religion Personal phone number Official phone number Residential address City Local Government Academic history Institutions Attended (Secondary, University and Others) Date Course of Study Duration of Course Certificate Obtained Grade Obtained Banking details Bank Name Account Number Bank Verification NO (BVN)	Recruitment processing Human capital management	Paper based forms (physical recruitment forms) Web forms (recruitment portal) Email (including electronic attachments)	SAP Servers and file cabinets or archiving systems, of all BU HR departments.

		Branch where the account was opened. Pension Fund Administrator PFA PIN Payer ID Number (TAX ID) Next of kin information Next of Kin and Phone No Beneficiary information Beneficiary and Phone No Name of Emergency Contact and Phone No Address of Emergency Contact Form of Identification (e.g. Driver's License, National Identity Card, Passport Page) Number of Children Name Gender Age Date of Birth 1st Nationality 2nd Nationality Emergency contact			
Human Resources	Reference Data	Referee's Name Place of Work Residential Address Email Relationship status Telephone Previous employer Name of organization Name of Supervisor Address Date of employment Date of leaving Current Position Entry position Email Phone No Current Compensation Entry compensation Academic Reference Name of Institution Course Graduation Year Department Address Email Contact Phone No Academic History Number of beneficiaries Name & Address of Beneficiary Relationship Percentage allotted. Bank account details	Processing of Employee benefit plan	Paper-based forms (Physical recruitment forms) Web forms (recruitment portal) Email (including electronic attachments)	SAP servers and file cabinets or archiving systems of all BU HR departments.
Human Resources	Beneficiary Information	Name of Legal Representative Address Telephone Number Name of Staff Staff Number Signature			