DATA PRIVACY POLICY

D'NAMAZ CAPITAL LIMITED

enquires@dnamazcapital.com

+234 916 444 1444

D'NAMAZ
CAPITAL LIMITED

Table of Contents

1. Introduction

Purpose of the Policy

D'Namaz Capital Limited ("DCL") is committed to safeguarding the privacy and personal data of its clients, suppliers, employees, and other stakeholders in accordance with the **NITDA Act 2023**, **NDPR 2022**, and global data protection standards. This policy outlines how we collect, use, store, and protect personal data to ensure transparency and trust.

At DCL, we recognize the critical importance of data privacy in fostering trust and maintaining strong relationships with our stakeholders. Our approach to data protection is built on transparency, accountability, and adherence to robust legal frameworks. By aligning our practices with the NITDA Act 2023 and NDPR 2022, as well as international data protection standards, we demonstrate our commitment to ensuring that all personal data is handled with the utmost care and security. This policy serves as a cornerstone of our operational philosophy, reflecting our dedication to safeguarding sensitive information and upholding the rights of data subjects.

We have instituted comprehensive measures to manage the lifecycle of personal data effectively, from collection and processing to storage and disposal. Our efforts are geared toward ensuring lawful, fair, and transparent data handling practices that align with the legitimate needs of our business operations. Through this policy, we aim to provide clarity to our stakeholders about how their data is managed, offering assurances of confidentiality, integrity, and compliance with regulatory requirements. By fostering an environment of trust, we strengthen our reputation as a responsible and forward-thinking organization.

Scope of Application

This Data Privacy Policy applies to all personal data processed by D'Namaz Capital Limited (DCL), covering the information of clients, employees, suppliers, partners, and other stakeholders. Regardless of the medium or format in which the data is collected, DCL is committed to maintaining the highest standards of data protection. Whether the data is obtained through traditional means such as physical forms, contracts, or verbal agreements, or through digital platforms like websites, mobile applications, and cloud-based services, this policy ensures that every piece of personal data is managed with diligence and care.

The scope of this policy extends to all types and formats of data, including written documents, electronic records, and verbal communications. DCL recognizes that personal data comes in many forms and is often shared across various channels. This policy ensures that no matter how the data is collected, stored, or transmitted, it is subject to the same robust measures for protection and management. By addressing both physical and digital data handling practices, DCL ensures comprehensive coverage of its operations, leaving no gaps in its approach to data privacy.

Through this policy, DCL establishes a unified and consistent framework for managing personal data across all its operations and interactions. This includes the implementation of stringent safeguards against unauthorized access, misuse, or data breaches. By applying the same high standards across all departments, locations, and functions, DCL aims to create an organization-wide culture of accountability and compliance with relevant data protection regulations.

Ultimately, this policy is designed to protect the rights and interests of all stakeholders involved with DCL. By fostering transparency and adhering to global best practices, DCL demonstrates its unwavering commitment to ethical data handling. This comprehensive scope ensures that every individual or organization that interacts with DCL can trust that their personal data is managed securely, responsibly, and in full compliance with applicable laws and regulations.

Legal and Regulatory Framework

DCL adheres to the following laws and regulations:

- Nigeria Data Protection Regulation (NDPR) 2022
- NITDA Act 2023
- Applicable global standards such as the General Data Protection Regulation (GDPR) for international compliance.

2. Definitions

- **Data Subject**: An individual whose personal data is processed. This includes clients, employees, suppliers, partners, or any other individual interacting with DCL whose information is collected, stored, or utilized.
- **Personal Data**: Any information relating to an identified or identifiable individual. This encompasses names, contact details, identification numbers, location data, online identifiers, and any factors specific to an individual's physical, physiological, genetic, mental, economic, cultural, or social identity.
- **Processing**: Any operation performed on personal data, including but not limited to collection, recording, organization, structuring, storage, retrieval, consultation, use, and disclosure by transmission, dissemination, or otherwise making available, alignment, combination, restriction, erasure, or destruction.

- **Data Controller**: D'Namaz Capital Limited (DCL), which determines the purposes and means of processing personal data and ensures that such processing complies with relevant regulations.
- **Data Processor**: Any third party, organization, or entity that processes personal data on behalf of DCL, following the company's instructions and data protection policies.
- **Consent**: The freely given, specific, informed, and unambiguous indication of an individual's agreement to the processing of their personal data through a clear affirmative action, such as a signature or ticking a box.
- **Data Breach**: A security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processed.
- **Data Retention**: The period during which personal data is stored by DCL, which is limited to the time necessary to fulfill the purposes for which the data was collected, unless otherwise required by law.
- **Data Minimization**: The principle that personal data collected must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- **Data Protection Impact Assessment (DPIA)**: A process undertaken to identify and minimize the data protection risks of a project, particularly when processing involves new technologies or poses high risks to the rights and freedoms of data subjects.
- **Anonymization**: The process of removing personal identifiers from data sets so that individuals cannot be identified, ensuring that privacy is preserved while enabling data use for research or analysis.
- **Pseudonymization**: A data processing technique that replaces or removes identifiable information from data sets to reduce re-identification risks, while still allowing data to be linked to the same data subject through additional information held separately.
- **Third Party**: Any individual, organization, or entity other than the data subject, data controller, or data processor that may receive, handle, or access personal data.

- **Sensitive Personal Data**: A special category of personal data requiring higher levels of protection due to its sensitive nature, such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health information, or data concerning a person's sex life or sexual orientation.
- **Data Subject Rights**: The legal rights afforded to individuals regarding their personal data, including the right to access, rectify, erase, restrict processing, data portability, object to processing, and not be subject to automated decision-making, as stipulated under applicable data protection regulations.

3. Principles of Data Protection

DCL abides by the following principles:

- **Lawfulness, Fairness, and Transparency**: Data is processed lawfully and transparently.
- **Purpose Limitation**: Data is collected for specified and legitimate purposes.
- **Data Minimization**: Only the data necessary for the purpose is collected.
- **Accuracy**: Data is kept accurate and up to date.
- **Storage Limitation**: Data is retained only as long as necessary.
- **Integrity and Confidentiality**: Data is protected against unauthorized access or breaches.

4. Types of Data Collected

a) **Client Data:** Name, contact information, identification documents, financial details, and transaction history.

b) **Supplier Data:** Company name, contact details, financial records, and contractual information.

c) **Employee Data:** Personal identification, employment history, medical records, and performance reviews.

d) **Other Stakeholder Data:** Data collected from website visitors, partners, and other affiliates.

5. Purpose of Data Collection and Processing

Data is collected to:

- Provide financial services and manage client portfolios.
- Fulfill legal and regulatory obligations.
- Enhance service delivery and client satisfaction.
- Facilitate communication and engagement with stakeholders.

6. Data Subject Rights

D'Namaz Capital Limited (DCL) is dedicated to protecting the rights of data subjects by adhering to the highest standards of data protection and privacy. The company recognizes the importance of these rights in fostering trust, transparency, and accountability in its data management practices. DCL actively ensures that individuals have full control over their personal data and that their rights are not only respected but also facilitated in accordance with applicable laws and regulations.

These rights, which form the cornerstone of ethical data handling, encompass various aspects designed to empower data subjects and guarantee their ability to access, manage, and safeguard their personal information. These rights include, but are not limited to, the following:

a) Data Access right

Data subjects have the fundamental right to access their personal data held by D'Namaz Capital Limited (DCL). This right ensures that individuals can obtain a clear understanding of the information DCL holds about them and how it is being used. It empowers individuals to verify the accuracy and completeness of their data, ensuring it is processed in a lawful, transparent, and fair manner. By enabling access, DCL fosters trust and transparency, reinforcing its commitment to respecting the privacy and rights of its stakeholders.

DCL has established a structured and efficient process for handling data access requests in the course of upholding this right.. Data subjects are provided with clear guidance on how to submit such requests, whether through a dedicated portal, email, or written communication. The process outlines the information that may be required to verify the identity of the requester, ensuring that personal data is disclosed only to the rightful individual. Additionally, DCL has committed to adhering to specific response timelines, reflecting its dedication to prompt and professional engagement with data subjects.

Through this approach, DCL not only complies with data protection laws but also demonstrates its proactive stance on safeguarding individual rights. The company’s transparent handling of access requests ensures that data subjects are kept informed about how their data is managed and processed, building confidence and trust in its data privacy practices. This right, coupled with DCL’s efficient processes, exemplifies its ongoing efforts to promote accountability and ethical data management across all levels of its operations.

b) Data Rectification

Data subjects have the right to request corrections or updates to their personal data when inaccuracies or incomplete information are identified. This right ensures that D'Namaz Capital Limited (DCL) maintains precise and reliable records, which are critical for lawful and effective data processing.

DCL supports transparency and reinforces the integrity of its data management practices by allowing individuals to rectify their information. Accurate data not only fulfills legal obligations but also builds trust and confidence among stakeholders, demonstrating DCL's commitment to ethical data handling.

DCL has also established clear and efficient mechanisms for submitting rectification requests, to facilitate the exercise of this right,. Data subjects can access user-friendly channels, such as online forms, email, or written submissions, to request updates to their personal information. The process is designed to be straightforward and accessible, ensuring that individuals can easily communicate their needs without unnecessary delays or barriers. Upon receiving such requests, DCL takes swift action to review, verify, and implement the necessary changes, thereby ensuring that its records remain up-to-date and accurate.

DCL underscores its commitment to respecting the rights of individuals and maintaining the highest standards of data integrity by prioritizing the accuracy of personal data, prompt and transparent handling of rectification requests not only ensures compliance with data protection regulations but also enhances stakeholder confidence in DCL’s processes. This proactive approach to data accuracy exemplifies the company’s dedication to fostering a culture of accountability and reliability in its data privacy practices.

c) Data Erasure

Data subjects have the right to request the deletion of their personal data under specific conditions, such as when the data is no longer required for its original purpose or when processing has become unlawful. Commonly known as the "right to be forgotten," this right empowers individuals to maintain control over their personal information and aligns with D'Namaz Capital Limited's (DCL) commitment to protecting individual privacy. By facilitating data erasure, DCL not only complies with legal obligations but also fosters transparency and trust in its data management practices.

Individuals can submit requests through designated channels, such as online forms or customer service portals, ensuring ease of access for all stakeholders to exercise this right. DCL has also implemented a clear and accessible process for handling erasure requests. Each request is thoroughly evaluated to confirm its validity under applicable laws and regulations, such as whether the data in question is still necessary or if other legal grounds for retention exist. DCL ensures that stakeholders are informed of the outcome of their requests, reinforcing its dedication to fairness and accountability in the management of personal data.

DCL demonstrates its commitment to ethical data practices and safeguarding individual rights by honoring legitimate data erasure requests, this proactive approach underscores the organization's focus on maintaining the privacy and dignity of its stakeholders while adhering to the highest standards of data protection. Through these efforts, DCL not only ensures compliance with regulatory frameworks but also strengthens the confidence of clients, employees, and other partners in its responsible data handling practices.

Process for Data Erasure at DCL

D'Namaz Capital Limited (DCL) can implement the following structured process for handling data erasure requests to ensure compliance with legal and ethical standards while safeguarding the rights of data subjects:

1. Submission of Data Erasure Request

- **Channels:** Establish accessible channels such as an online portal, dedicated email address, or physical submission form for receiving erasure requests.
- **Required Information:** Provide a standard request form that captures essential details, including:
    - Name and contact information of the requester.
    - Description of the personal data to be erased.
    - Reason for the erasure request (e.g., no longer necessary, consent withdrawal, or unlawful processing).
- **Acknowledgment:** Send an acknowledgment receipt to the data subject within a specified timeframe (e.g., 3 business days).

2. Verification of Identity and Request

- **Identity Confirmation:** Verify the identity of the requester to prevent unauthorized data access or deletion. This can include requiring government-issued IDs or matching request details against existing records.
- **Validity Check:** Assess the validity of the request under applicable laws, such as GDPR or NDPR, ensuring conditions like data no longer being necessary or unlawful processing are met.
- **Notification:** If the request is invalid, inform the requester with a clear explanation and details on alternative actions, if applicable.

3. Internal Review and Evaluation

- **Assessment:** Conduct a thorough review of the data involved to determine if it qualifies for deletion. This includes checking:
    - Legal grounds for retaining the data (e.g., ongoing contracts or regulatory compliance).
    - Third-party processing agreements and data locations (e.g., cloud storage or external databases).
- **Documentation:** Maintain records of all requests and evaluations to demonstrate compliance during audits or regulatory inquiries.

4. Execution of Data Erasure

- **Data Deletion:** Perform secure deletion methods appropriate to the medium (e.g., digital deletion for electronic records and shredding for physical copies).
- **Third-Party Notification:** Inform any third-party processors or controllers to erase the data from their systems, ensuring complete removal across all platforms.
- **Data Backup:** If data exists in backup systems, develop procedures to ensure erasure during the next backup cycle unless exempt under legal requirements.

5. Confirmation and Follow-Up

- **Confirmation Letter:** Provide the data subject with a confirmation once the data has been deleted. Include a summary of the actions taken and any exceptions (e.g., data retained due to legal obligations).
- **Timeline Adherence:** Complete the entire process within the legally mandated timeframe (e.g., one month under GDPR) or as per internal policies.
- **Feedback Mechanism:** Offer a feedback mechanism for the requester to ensure satisfaction with the resolution process.

6. Periodic Review of the Erasure Process

- **Policy Updates:** Regularly review and update the data erasure process to reflect changes in laws, technology, and business practices.

- **Training:** Conduct staff training to ensure consistent and compliant handling of erasure requests.
- **Audits:** Perform periodic audits to verify adherence to the policy and identify areas for improvement.

This comprehensive approach ensures that DCL respects the rights of data subjects while maintaining compliance with regulatory requirements and fostering trust among stakeholders.

d) Withdrawal of Consent

Data subjects have the right to withdraw their consent for data processing at any time, thereby exercising control over their personal data. This right empowers individuals to make decisions about their data usage, particularly when they no longer wish for their data to be processed for specific purposes. DCL acknowledges this right and has established user-friendly mechanisms to facilitate the withdrawal process seamlessly.

Withdrawal of consent does not affect the lawfulness of processing that occurred prior to the withdrawal, ensuring compliance with regulatory standards. DCL ensures that the withdrawal process is transparent, accessible, and efficient, allowing data subjects to submit their requests without undue burden. By upholding this right, DCL reaffirms its dedication to respecting individual choices and maintaining ethical data management practices in alignment with global standards.

Process for Withdrawal of Consent at DCL

To ensure that D'Namaz Capital Limited (DCL) respects the right of data subjects to withdraw consent and complies with applicable data protection regulations, the following structured process is recommended:

1. Submission of Consent Withdrawal Request

- **Channels:** Provide accessible channels for submitting withdrawal requests, such as an online portal, email address, customer service line, or physical submission forms.
- **Request Form:** Develop a standard withdrawal form capturing essential details, including:
    - Name and contact information of the data subject.
    - Specific consent(s) to be withdrawn (e.g., marketing communications, data sharing).
    - Reason for the withdrawal (optional).
- **Acknowledgment:** Send an acknowledgment receipt to the data subject within a specified timeframe (e.g., 3 business days), confirming receipt of the request.

2. Verification of Identity and Request

- **Identity Confirmation:** Verify the requester's identity to prevent unauthorized actions. Acceptable methods may include matching data subject information with existing records or requiring government-issued identification.
- **Request Scope:** Clearly define the scope of consent withdrawal to ensure that specific consents (e.g., for certain activities or purposes) are accurately identified.
- **Notification:** If the request cannot be fulfilled (e.g., data is processed under a legal obligation), promptly notify the requester with a clear explanation and details of their rights.

3. Internal Review and Assessment

- **Review Processing Activities:** Identify all activities and systems where the subject's data is processed under the withdrawn consent.
- **Evaluate Impact:** Determine whether the withdrawal of consent affects any ongoing activities and identify alternate lawful bases for processing if applicable (e.g., legal obligations or contractual requirements).
- **Documentation:** Maintain detailed records of consent withdrawals and the actions taken to demonstrate compliance with data protection laws during audits or inquiries.

4. Execution of Consent Withdrawal

- **Cessation of Processing:** Immediately cease all processing activities that relied solely on the withdrawn consent.
- **System Updates:** Update all relevant systems, databases, and communication channels to reflect the change in consent status.
- **Third-Party Notification:** Inform all third parties or processors relying on the withdrawn consent to cease data processing for the specified purposes.

5. Confirmation and Follow-Up

- **Confirmation Letter:** Notify the data subject once the withdrawal has been processed. Include details of actions taken, such as stopping specific data uses or communications.

- **Timeline Adherence:** Ensure the entire withdrawal process is completed within the legally mandated timeframe (e.g., one month under GDPR or NDPR).
- **Feedback Mechanism:** Provide a channel for data subjects to offer feedback on their experience with the withdrawal process, fostering trust and improving services.

6. Periodic Review and Process Optimization

- **Policy Updates:** Regularly review and update withdrawal procedures to align with changes in laws, regulations, and best practices.
- **Employee Training:** Conduct regular training sessions for employees to ensure consistent and efficient handling of withdrawal requests.
- **Audits:** Periodically audit the withdrawal process to identify areas for improvement and ensure compliance with data protection regulations.

e) Right to Objection

Data subjects have the right to object to the processing of their personal data for specific purposes, such as direct marketing, profiling, or any other activities that may have an impact on their privacy or personal interests. This right empowers individuals to exercise control over their data, ensuring that it is not used in ways they find objectionable or invasive. By providing this mechanism, DCL underscores its commitment to respecting individual autonomy and promoting ethical data practices in alignment with legal and regulatory frameworks.

To facilitate the exercise of this right, DCL has implemented a structured and user-friendly process for data subjects to raise objections. Data subjects can submit their objections through various channels, such as email, online forms, or in writing. Upon receipt of an objection, DCL promptly acknowledges the request and initiates a thorough evaluation of the processing activities in question. This evaluation involves assessing whether the objection is valid under applicable laws and whether the processing activity has a legitimate basis that may override the data subject's rights, such as contractual or legal obligations.

DCL ensures that all objections are addressed fairly and transparently, with a strong emphasis on protecting the rights and privacy of data subjects. If the objection is upheld, DCL takes immediate action to cease the specific processing activity, updating its systems and notifying any relevant third parties involved in the data processing. This commitment to respecting objections fosters trust among stakeholders, reinforces DCL's dedication to ethical data management, and ensures ongoing compliance with data protection regulations.

Process for Exercising the Right to Object at DCL

To ensure that data subjects can effectively exercise their right to object to the processing of their personal data, D'Namaz Capital Limited (DCL) has established the following structured process:

1. Submission of Objection Request

- **Channels for Submission:** Data subjects may submit their objections through multiple channels, including:
    - An online portal or dedicated web form on DCL's website.
    - A designated email address for privacy-related requests.
    - Physical mail to DCL's data protection office.
- **Required Information:** The objection request should include:
    - Full name and contact details of the data subject.
    - Specific details of the processing activity being objected to (e.g., direct marketing, profiling).
    - Reason for the objection (optional but recommended to facilitate assessment).
- **Acknowledgment:** DCL will acknowledge receipt of the request within 3 business days, providing a reference number for tracking purposes.

2. Verification and Validation of Request

- **Identity Verification:** To prevent unauthorized actions, DCL will verify the identity of the data subject through appropriate measures, such as confirming details against existing records or requesting identification documents.
- **Request Scope Review:** The scope of the objection is carefully reviewed to understand the processing activity in question and the basis of the objection. This step ensures that DCL can accurately assess the validity and implications of the request.

3. Internal Review and Assessment

- **Legal and Regulatory Compliance:** DCL assesses whether the objection aligns with the rights provided under applicable laws and whether the processing activity in question is lawful and justified.

- **Impact Analysis:** If the processing is based on legitimate interests, DCL evaluates whether those interests override the data subject's rights and freedoms. For objections related to direct marketing, processing will cease upon validation of the objection.
- **Consultation:** Relevant departments, such as legal or compliance teams, may be consulted to ensure that the decision-making process is thorough and in line with regulatory requirements.

4. Response and Action

- **Decision Notification:** DCL will communicate the outcome of the review to the data subject within the legally mandated timeframe (typically one month). The response will include:
  - The decision (approval or rejection of the objection).
  - Details of the actions taken or reasons for rejecting the objection.
- **Execution of Changes:** If the objection is upheld, DCL will:
  - Cease the relevant processing activities immediately.
  - Update internal systems and notify any third parties involved in the processing to take similar action.

5. Record-Keeping and Continuous Improvement

- **Documentation:** Maintain detailed records of all objection requests and actions taken to demonstrate compliance with data protection regulations during audits or inquiries.
- **Feedback Mechanism:** Provide data subjects with a channel to offer feedback on the objection process, enabling DCL to improve its procedures.
- **Periodic Review:** Regularly review and update the objection-handling process to ensure alignment with evolving legal requirements and best practices.

f) Data Portability

Data subjects have the right to request and obtain a copy of their personal data in a structured, commonly used, and machine-readable format. This right enables individuals to transfer their data to another organization or use it for their own purposes without any hindrance. DCL recognizes the importance of this right in empowering data subjects with greater control over their information.

DCL has developed robust procedures and tools to facilitate data portability requests, to ensure the seamless exercise of this right. By providing personal data in a standardized and accessible format, DCL supports the interoperability of data across different systems and organizations. This commitment underscores DCL's dedication to fostering transparency, accountability, and respect for individual rights in all aspects of its data management practices.

7. Data Collection and Consent

Methods of Collection

a) Online Forms

DCL utilizes secure online forms to collect personal data efficiently and transparently. These forms are hosted on company websites, mobile platforms, and other digital interfaces. Designed with user-friendliness in mind, they enable individuals to provide the necessary information seamlessly. The forms typically include fields for essential details such as names, contact information, and other relevant data, depending on the purpose. The use of encryption and secure protocols ensures the confidentiality and integrity of the data submitted through these channels.

Moreover, DCL ensures that all online forms are compliant with legal and regulatory standards, incorporating clear privacy notices and consent mechanisms. Users are informed about the purpose of data collection, how their data will be used, and their rights. This transparency helps build trust while enabling DCL to meet its obligations under the NITDA Act 2023 and NDPR 2022. Regular audits and updates to these forms ensure that they remain effective and aligned with evolving privacy standards.

b) In-Person Interactions

Personal data is often collected during in-person interactions between DCL representatives and stakeholders. These interactions may occur at company offices, events, or during on-site visits, providing an opportunity to gather detailed and context-specific information. In such scenarios, data is typically recorded on physical forms, electronic devices, or through direct input into secured systems.

To maintain privacy and security, DCL ensures that all in-person data collection processes are conducted in adherence to strict confidentiality protocols. Stakeholders are informed about the purpose of data collection, and their consent is obtained before proceeding. Training is provided to DCL staff to handle personal data responsibly, emphasizing the importance of maintaining privacy during and after data collection. By prioritizing transparency and accountability in in-person interactions, DCL fosters a culture of trust and compliance.

c) Mobile Apps

DCL leverages mobile applications to facilitate convenient and efficient data collection from its clients, employees, and other stakeholders. These apps are equipped with features that allow users to submit personal information, access services, and interact with DCL seamlessly. Data collected through mobile apps is encrypted and stored securely, ensuring protection against unauthorized access.

To enhance transparency, DCL incorporates detailed privacy policies and consent forms within its mobile applications. Users are provided with clear information on how their data will be used, stored, and shared, ensuring informed decision-making. The apps are regularly updated to incorporate the latest security measures and comply with applicable privacy regulations. By integrating robust data protection measures, DCL ensures that mobile app users can interact with the company confidently and securely.

d) Third-Party Integrations

DCL also collects data through third-party integrations, including partnerships with service providers, payment gateways, and other external platforms. These integrations facilitate seamless operations, such as processing transactions, verifying identities, and enhancing user experiences. Data collected through these channels is subject to strict contractual agreements that ensure compliance with privacy laws and standards.

DCL carefully selects third-party partners based on their commitment to data protection and privacy. All data exchanged is encrypted and securely transmitted to prevent unauthorized access. Additionally, DCL conducts periodic reviews and assessments of third-party integrations to ensure ongoing compliance and mitigate potential risks. This approach underscores DCL's dedication to maintaining the highest standards of data privacy while leveraging external resources to enhance its operations.

7. Data Collection Consent Mechanisms (DCCM)

At D'Namaz Capital Limited (DCL), we prioritize transparency and accountability in how we handle personal data. Our consent mechanism is a critical part of our commitment to ethical data practices, ensuring that stakeholders, including customers, employees, and partners, have control over their personal information. We obtain consent in a clear and straightforward manner, providing comprehensive details about the purpose and use of the data being collected.

Consent is always specific, voluntary, and can be withdrawn at any time without impacting the relationship or the validity of prior data usage. This approach reflects our dedication to building trust with our stakeholders while maintaining compliance with all relevant data protection regulations. Your privacy is central to everything we do. This includes;

a) Explicit Consent for Sensitive Data

DCL requires explicit consent from individuals before processing any sensitive personal data, such as health information, financial records, or biometric details. This ensures that data subjects are fully aware of the specific purposes for which their sensitive data is being collected and processed. The consent process includes clear explanations, allowing individuals to make informed decisions about their data. DCL employs robust consent documentation mechanisms, such as signed agreements or electronic confirmations, to provide a record of compliance.

In addition, DCL emphasizes transparency throughout the consent process. Individuals are provided with detailed information about their rights, including the ability to withdraw consent at any time. By adhering to these practices, DCL ensures compliance with the NITDA Act 2023, NDPR 2022, and other relevant global data protection standards, fostering trust and accountability in handling sensitive personal data.

b) Opt-In and Opt-Out Mechanisms for Marketing Communications

DCL implements opt-in and opt-out mechanisms for marketing communications. Before sending any promotional materials, newsletters, or offers, to respect the privacy preferences of data subjects, DCL ensures that individuals have explicitly opted in to receive such communications. The opt-in process involves clear and straightforward options, allowing individuals to grant or withhold their consent easily.

For those who wish to discontinue receiving marketing communications, DCL provides user-friendly opt-out mechanisms. These include options such as "unsubscribe" links in emails or a simple process to update preferences through customer portals. DCL processes opt-out requests promptly and ensures that no further marketing communications are sent to individuals who have withdrawn their consent. This approach reinforces DCL's commitment to respecting individual privacy and maintaining compliance with legal and regulatory requirements.

8. Data Usage and Sharing

a) Purpose Limitation

DCL is committed to the principle of purpose limitation, ensuring that personal data collected is used solely for the specific purposes outlined in this policy. These purposes are transparently communicated to data subjects at the point of data collection to establish trust and clarity. Data is processed strictly within the confines of its intended use, whether for fulfilling contractual obligations, legal compliance, or improving service delivery. Any deviation from the original purpose requires obtaining additional consent from the data subjects, emphasizing DCL's dedication to ethical data practices.

By adhering to the purpose limitation principle, DCL minimizes risks associated with unauthorized or unintended data usage. Regular reviews and audits are conducted to ensure that data processing activities align with stated purposes. This approach not only safeguards the rights of data subjects but also upholds DCL's compliance with the NITDA Act 2023, NDPR 2022, and other global data protection standards. Maintaining this focus fosters accountability and reinforces confidence in DCL's data management practices.

b) Third-Party Data Sharing

DCL shares personal data with third parties only when it is necessary to facilitate service delivery or comply with legal obligations. Before sharing any data, DCL ensures that robust agreements are in place with third-party service providers to uphold the privacy and security of the data. These agreements mandate compliance with applicable data protection regulations, including the NITDA Act 2023 and NDPR 2022, thereby safeguarding the interests of data subjects.

DCL's approach to third-party data sharing is guided by a principle of minimalism, sharing only the data required to achieve the intended purpose. The company also conducts due diligence to verify that third-party entities have appropriate security measures and policies in place. Regular monitoring and audits are conducted to assess the third parties' adherence to data protection standards, ensuring that the shared data remains secure and is not misused. By maintaining this level of oversight, DCL builds trust with stakeholders and reinforces its commitment to ethical and responsible data sharing practices.

c) Cross-Border Data Transfers

DCL ensures that all cross-border data transfers comply fully with the requirements outlined in the NDPR and other relevant international data protection regulations. Before transferring data to jurisdictions outside Nigeria, DCL confirms that the destination country has adequate data protection laws or that appropriate safeguards, such as binding corporate rules or standard contractual clauses, are in place. These measures aim to protect the integrity and confidentiality of the data while upholding the rights of data subjects.

To further ensure compliance, DCL performs comprehensive assessments of the legal frameworks and security measures of recipient entities involved in cross-border transfers. The company also informs data subjects about potential international transfers and obtains explicit consent where necessary. Regular audits and monitoring processes are employed to verify adherence to these standards, ensuring that data remains secure and is processed in accordance with its intended purpose. By implementing these rigorous protocols, DCL maintains transparency and trust in handling cross-border data transfers.

9. Data Security and Protection

9.1 Data Security Measures

a) Encryption of Sensitive Data

DCL employs advanced encryption technologies to protect sensitive data both in transit and at rest. This ensures that unauthorized parties cannot access or decipher the data, maintaining its confidentiality and integrity. Encryption protocols adhere to industry standards, including AES-256 for data storage and TLS for secure communications. By prioritizing encryption, DCL minimizes the risks of data breaches and unauthorized disclosures.

Additionally, encryption mechanisms are applied uniformly across all data repositories and communication channels. This includes databases, email systems, and file storage services. DCL regularly updates its encryption algorithms to align with technological advancements and emerging security threats, guaranteeing the ongoing security of sensitive information. Employees and partners are also trained to handle encrypted data appropriately, reinforcing organizational security measures.

To enhance transparency, DCL maintains detailed records of encryption processes and incidents involving encrypted data. These records are regularly audited to ensure compliance with regulatory requirements and internal policies. By integrating encryption into its core data protection framework, DCL demonstrates its commitment to safeguarding sensitive data against evolving cyber threats.

b) Multi-Factor Authentication for System Access

Access to DCL's systems and platforms is secured through multi-factor authentication (MFA), which requires users to verify their identity using multiple credentials. This robust security measure combines factors such as passwords, biometric verification, and one-time passcodes, significantly reducing the risk of unauthorized access. MFA is enforced across all critical systems, ensuring only authorized personnel can access sensitive data.

DCL implements MFA as part of its broader identity and access management strategy. Regular reviews and updates are conducted to optimize authentication processes, incorporating the latest advancements in security technologies. Employees are provided with clear guidelines and training on the importance of MFA, fostering a culture of vigilance and responsibility. In addition, system logs are monitored to detect and respond to any suspicious login attempts promptly.

MFA is also extended to external stakeholders, including clients and suppliers, who access DCL's online platforms. This ensures a consistent security standard across the organization's digital ecosystem. By integrating MFA into its security framework, DCL not only enhances data protection but also instills confidence among stakeholders regarding the safety of their personal information.

c) Regular Security Audits and Penetration Testing

DCL conducts regular security audits and penetration testing to identify vulnerabilities and strengthen its cyber security infrastructure. These proactive measures help uncover weaknesses in systems, networks, and applications, enabling the organization to address potential threats before they are exploited. Security audits are conducted in alignment with industry standards and regulatory requirements, ensuring a comprehensive evaluation of the organization's defenses.

Penetration testing involves simulating real-world cyber-attacks to assess the resilience of DCL's security measures. These tests are performed by certified cybersecurity professionals who provide actionable insights into areas requiring improvement. The findings from these tests guide the implementation of targeted enhancements, such as patching vulnerabilities and optimizing system configurations.

In addition to technical assessments, DCL incorporates employee awareness programs into its audit framework. These programs educate staff on recognizing and mitigating cyber threats, creating an additional layer of defense. By combining rigorous audits, penetration testing, and employee training, DCL builds a resilient security posture capable of adapting to the dynamic cybersecurity landscape.

9.2 Data Protection

At D'Namaz Capital Limited (DCL), data protection within our data security management system ensures confidentiality, integrity, and availability of personal information. We implement safeguards like encryption, multi-factor authentication, and access controls to prevent unauthorized access or data loss. Regular audits and compliance checks identify vulnerabilities, while continuous monitoring ensures rapid threat response. By fostering awareness and accountability among stakeholders, DCL upholds privacy rights, builds trust, and maintains the highest standards of data security in compliance with regulatory requirements. This includes;

9.2.1 Data Breach Management

Data Breach Management refers to the structured approach that D'Namaz Capital Limited (DCL) employs to address incidents where personal data may be exposed, lost, or accessed without authorization. In alignment with the NITDA Act 2023 and NDPR 2022, DCL ensures swift action to contain breaches, assess their scope, and mitigate harm.

Key steps include activating a response team to secure affected systems, notifying impacted data subjects and regulatory authorities transparently, and implementing corrective measures to prevent recurrence. By integrating these practices, DCL upholds its commitment to safeguarding personal data and fostering trust with clients, suppliers, employees, and stakeholders. This also includes;

a) Immediate Containment and Assessment

In the event of a data breach, DCL initiates immediate measures to contain the breach and prevent further unauthorized access to data. A dedicated response team is activated to assess the scope and impact of the breach, identifying affected systems and data. These initial steps are critical for mitigating potential harm and ensuring the organization can respond effectively. The response team works closely with IT specialists to isolate compromised systems and implement interim security measures to safeguard unaffected data.

This containment phase also involves documenting all actions taken and evidence collected for investigative and reporting purposes. By acting swiftly, DCL demonstrates its commitment to protecting the interests of data subjects and maintaining compliance with regulatory requirements. Regular training ensures that all employees understand their roles during a breach, enabling a coordinated and efficient response.

b) Notification to Affected Data Subjects and Regulatory Authorities

DCL prioritizes transparency in its breach management approach by promptly notifying affected data subjects and regulatory authorities, as required by the NDPR and other applicable laws. Notifications include a clear explanation of the breach, the type of data involved, potential risks, and recommended steps for individuals to mitigate harm. By providing timely information, DCL empowers data subjects to take proactive measures to protect themselves.

For regulatory compliance, DCL ensures that breach notifications are submitted within the stipulated timelines, detailing the actions taken to address the breach and prevent recurrence. This transparent communication reinforces trust between DCL, its stakeholders, and regulatory bodies. Comprehensive records of notifications are maintained as part of DCL’s commitment to accountability and continuous improvement.

c) Corrective Actions to Prevent Recurrence

DCL conducts a thorough investigation to determine the root cause and implement corrective actions, after addressing the immediate effects of a breach. This process includes reviewing existing security measures, updating protocols, and strengthening system defenses to mitigate future risks. Lessons learned from the breach are integrated into the organization's data protection framework, enhancing its resilience against similar incidents.

Corrective actions also involve training employees on updated security practices and emphasizing the importance of vigilance in data handling. DCL fosters a culture of continuous improvement by regularly revisiting and refining its breach management procedures. By taking proactive and comprehensive steps to prevent recurrence, DCL reaffirms its dedication to safeguarding personal data and upholding the highest standards of data security.

10. Data Retention and Disposal

a) Data Retention Periods

D'Namaz Capital Limited (DCL) adopts a clear and compliant data retention policy to ensure that personal data is stored only for as long as it is legally or operationally necessary. Retention periods are defined based on the type of data, its purpose, and regulatory requirements, ensuring adherence to the NITDA Act 2023 and NDPR 2022. For instance, financial records may be retained for a statutory period, while marketing data is kept only as long as consent remains valid. By implementing such precise timelines, DCL balances operational efficiency with privacy compliance.

This approach minimizes unnecessary data storage, thereby reducing the risk of unauthorized access or misuse. The retention schedule is regularly reviewed and updated to align with evolving regulations and organizational needs. Stakeholders are informed of these practices to enhance transparency and build trust.

b) Secure Disposal Methods

Once data is no longer required for legal or operational purposes, DCL ensures its secure disposal through methods such as data anonymization, encryption-based shredding, or physical destruction for hard copies. This process is guided by stringent protocols to prevent unauthorized recovery or misuse of disposed data. The organization engages certified disposal vendors when necessary to handle sensitive information professionally and securely.

Employees are trained on the importance of secure disposal practices to foster a culture of accountability and compliance. Regular audits are conducted to verify that disposal procedures are consistently followed, further reinforcing the organization's commitment to robust data protection.

c) Balancing Retention and Privacy

At D'Namaz Capital Limited (DCL), balancing data retention and privacy is a key principle of our Data Retention and Disposal Policy, reflecting our commitment to safeguarding stakeholder information while meeting operational and regulatory requirements.

Data retention involves maintaining personal and organizational data for as long as it is necessary to achieve specific, legitimate purposes, such as fulfilling contractual obligations, complying with legal mandates, or supporting business operations. However, retaining data beyond its usefulness poses privacy risks, including potential breaches or misuse. To address this, DCL implements retention schedules aligned with legal standards and industry best practices, ensuring that data is kept only for the minimum period required to serve its intended purpose.

Equally important is our focus on data disposal to uphold privacy and mitigate risks associated with unnecessary data storage. Once data is no longer needed, it is securely and permanently destroyed or anonymized, depending on its nature and relevance. DCL employs robust disposal procedures, including encryption, secure shredding, and digital wiping, to prevent unauthorized access during the deletion process. By carefully balancing retention and privacy, DCL not only complies with applicable data protection regulations but also builds trust with stakeholders, ensuring their information is handled responsibly and with the utmost respect for privacy.

11. Responsibilities and Accountability

11.1 Data Protection Officer (DPO)

The Data Protection Officer (DPO) at D'Namaz Capital Limited ("DCL") plays a pivotal role in ensuring that the company remains compliant with data protection laws and regulations. The DPO is tasked with overseeing all aspects of data protection within the organization, ensuring that personal data is handled responsibly, and safeguarding the rights of data subjects. This role is essential in promoting privacy awareness across the company and ensuring that data protection practices are consistently followed.

11.2 Key Functions of the Data Protection Officer (DPO):

- **Compliance Oversight**:
    - Ensures that DCL complies with all applicable data protection laws, regulations, and industry standards, such as the GDPR or Nigeria's Data Protection Regulation (NDPR).
    - Develops, implements, and reviews data protection policies to ensure they are up-to-date with the latest regulations.
- **Data Protection Inquiries**
    - Serves as the primary contact for data subjects and authorities regarding data protection concerns, including inquiries about how personal data is being used.
    - Investigates and responds to complaints and requests related to data protection from employees, clients, or third parties.

- **Monitoring and Reporting**:
  - Monitors the effectiveness of data protection measures across the organization and reports any risks, breaches, or non-compliance issues to senior management.
  - Conducts regular audits and assessments of data processing activities to ensure compliance.
- **Risk Assessment**:
  - Identifies and assesses risks related to data processing operations, including evaluating potential data protection impacts on new projects or services.
  - Provides recommendations to mitigate data protection risks, ensuring that privacy considerations are embedded in business processes.
- **Training and Awareness**:
  - Develops and conducts training programs to educate staff on data protection principles and their responsibilities under the company's privacy policy.
  - Ensures that employees are aware of their obligations regarding the handling of personal data.
- **Protection of Data Subject Rights**:
  - Ensures that the rights of data subjects (such as access, rectification, erasure, and data portability) are respected and that requests are handled in a timely manner.
  - Facilitates the process for individuals to exercise their rights over their personal data.
- **Incident Management**:
  - Leads the response to data protection incidents, including data breaches, ensuring that the appropriate steps are taken to mitigate damage and notify relevant authorities and affected individuals, where required.
  - Maintains records of any data breaches and ensures that corrective actions are taken to prevent recurrence.

By fulfilling these responsibilities, the DPO ensures that DCL's operations align with data protection standards, fostering trust with clients and stakeholders while mitigating legal risks associated with data privacy violations.

11.3 Employee Responsibilities

At D'Namaz Capital Limited ("DCL"), safeguarding data privacy is not just a regulatory requirement but a core aspect of our organizational integrity and operational excellence. Employees play a critical role in ensuring that data protection protocols are adhered to, helping to secure the trust of our clients, partners, and stakeholders. This document outlines specific responsibilities that all employees must uphold to maintain compliance with our Data Protection and Privacy Policy.

- **Data handling in Accordance with Data Privacy Policy**

Employees are required to strictly adhere to the data handling protocols outlined in this policy. This includes the secure collection, storage, processing, and disposal of data in a manner that aligns with applicable data protection regulations, such as the General Data Protection Regulation (GDPR) or the Nigerian Data Protection Regulation (NDPR). Employees must ensure that all personal and sensitive data is accessed only by authorized personnel and used solely for its intended purpose.

Additionally, employees must take proactive steps to prevent unauthorized access to data by using secure passwords, encryption, and other technological safeguards provided by the company. Routine training sessions will equip employees with knowledge of the latest tools and practices for secure data handling. Non-compliance with these standards may result in disciplinary action, up to and including termination of employment.

Employees must also remain vigilant and avoid careless practices that could compromise data security. This includes refraining from sharing sensitive data over unsecured communication channels, accessing company data on public or unprotected networks, or leaving documents containing sensitive information unattended. By maintaining strict control over data access and usage, employees help protect the company's reputation and legal standing.

- **Report Potential Breaches Immediately**

In the event of a suspected or actual data breach, employees are obligated to report the incident immediately to the designated Data Protection Officer (DPO) or their direct supervisor. Timely reporting is essential to initiate mitigation measures, limit potential damage, and comply with regulatory requirements for breach notification. Employees must familiarize themselves with the reporting channels and procedures to ensure swift action in such situations.

Reporting a breach includes providing as much detail as possible, such as the nature of the breach, the type of data affected, and the individuals or systems involved. This information helps the company assess the risk, determine whether notification to affected parties or authorities is required, and implement corrective actions. Employees should never attempt to conceal or address

a breach on their own, as this could exacerbate the issue or lead to non-compliance with reporting obligations.

DCL encourages a culture of openness and accountability in handling potential breaches. Employees are assured that reporting a breach in good faith will not result in punitive measures against them. Instead, prompt reporting will be recognized as a vital contribution to maintaining the company's data protection standards and fostering trust with clients and stakeholders. By fulfilling these responsibilities, employees at DCL actively contribute to creating a secure environment that prioritizes the protection of personal and organizational data.

12. Compliance with NITDA Act 2023 and NDPR 2022

At D'Namaz Capital Limited (DCL), compliance with the NITDA Act 2023 and the Nigerian Data Protection Regulation (NDPR) 2022 is foundational to our data governance framework. The company ensures full adherence to these regulations by implementing structured processes that govern how data is collected, processed, stored, and shared. This includes maintaining detailed records of processing activities to track how personal data is handled across the organization. These records serve as an essential compliance tool, demonstrating DCL's commitment to transparency and accountability in data processing operations, while also enabling swift responses to inquiries from stakeholders or regulatory bodies.

In alignment with the NITDA Act and NDPR, DCL routinely conducts Data Protection Impact Assessments (DPIAs) for new projects, technologies, or processes that involve significant data handling. These assessments evaluate potential risks to the privacy and security of personal data and help identify mitigative measures to address those risks effectively. By integrating DPIAs into our operational workflow, DCL ensures proactive risk management and compliance with regulatory requirements, fostering a culture of trust and responsibility. This approach not only safeguards the rights of data subjects but also reinforces the company's reputation as a responsible and compliant entity.

Furthermore, DCL actively cooperates with regulatory authorities, including the National Information Technology Development Agency (NITDA), to ensure seamless compliance with the evolving legal landscape. The company provides timely reports, facilitates audits, and addresses regulatory inquiries as required under the NITDA Act and NDPR. This open and collaborative approach enables DCL to remain updated on best practices and regulatory changes, ensuring continuous alignment with data protection standards. By maintaining an active partnership with regulators, DCL underscores its dedication to upholding the highest standards of data protection and privacy.

13. Review and Updates to the Policy

At D'Namaz Capital Limited (DCL), the Data Protection and Privacy Policy is subject to regular review and updates to ensure it remains aligned with the latest legal, regulatory, and operational requirements. This policy is reviewed annually, providing a structured timeline to assess its relevance and effectiveness in safeguarding personal data. The review process includes a comprehensive evaluation of emerging data protection laws, advancements in technology, and industry best practices, ensuring the policy stays current and robust against potential data security risks.

In addition to the scheduled annual review, the policy is updated as necessary to address changes in regulatory frameworks, such as amendments to the NITDA Act or the Nigerian Data Protection Regulation (NDPR). Adjustments are also made to reflect shifts in DCL's business operations, including the introduction of new products, services, or technological tools that involve data handling. These updates are critical in maintaining compliance and ensuring that employees, stakeholders, and partners are aware of their responsibilities under the evolving policy.

DCL prioritizes transparency and communication during policy reviews and updates. Stakeholders, including employees and partners, are notified of significant changes through internal communications, training sessions, or formal notices. This ensures that everyone involved is informed and equipped to comply with the updated requirements. By committing to an adaptive and proactive approach, DCL demonstrates its dedication to maintaining the integrity of its data protection practices and fostering a secure environment for all stakeholders.

14. Appendices

- Appendix A: Consent Form Template
- Appendix B: Data Breach Incident Report Template
- Appendix C: Employee Data Handling Guidelines

D'NAMAZ CAPITAL LIMITED

Consent Form for Data Collection

1. Purpose of Data Collection

D'Namaz Capital Limited (DCL) collects your personal data for the purpose of……. [Describe purpose – e.g., marketing, customer support, etc.]. This information will be processed in compliance with the Data Protection and Privacy Policy of DCL and applicable data protection laws.

2. Data to be collected

The types of personal data we collect may include:

- Full name
- Contact information (phone number, email address)
- Date of birth
- [Additional data types]: Specify

3. Consent Declaration

I, the undersigned, hereby consent to the collection, processing, and storage of my personal data for the purposes described above. I understand that I have the right to withdraw my consent at any time by contacting DCL, and that this will not affect the legality of any processing done before the withdrawal.

- **Full Name:** ……
- **Signature:**…….....
- **Date:** ……

4. Withdrawal of Consent

To withdraw your consent, please contact ……. All personal data collected prior to the withdrawal of consent will be handled in accordance with DCL's Data Protection and Privacy Policy.

Company Stamp

Staff Name & Date executed ……..……

D'NAMAZ CAPITAL LIMITED

N.B: This form cannot be executed by Proxy.

D'NAMAZ CAPITAL LIMITED

Data Breach Incident Report

Date of Incident: _____

Reported By: _____

Department: _____

Details of the Breach

- **Type of Data Involved:** [e.g., personal data, financial data, etc.] _____

  _____
- **Nature of the Breach:** [Briefly describe the breach – e.g., unauthorized access, data loss, theft, etc.] _____

  _____
- **Number of Affected Individuals:** [e.g., 100 clients, 5 employees, etc.] _____
- **Date and Time of Discovery:** [Insert Date and Time] _____

Actions Taken

- **Immediate Actions Taken:** [e.g., access blocked, data secured, etc.] _____

  _____
- **Notified Authorities:** [e.g., NITDA, affected individuals, etc.] _____
- **Investigation Details:** [e.g., cause of breach, persons involved, etc.]_____

  _____
- **Remediation Measures:** [e.g., additional security protocols, training, etc.]

  _____

Future Prevention Measures

- [Describe any changes to procedures, training, or technologies to prevent future breaches.]_____

  _____

Report Submitted By: _____

Reviewed By: _____

Date of Review: _____

D'NAMAZ CAPITAL LIMITED

Employee Data Handling Guidelines

The Employee Data Handling Guidelines provide clear instructions for employees on how to securely handle personal data within the company. Below is the recommended structure:

1. Data Access Control

- Employees should access personal data only if necessary for their role.
- Access to sensitive or confidential data should be restricted to authorized personnel.
- Ensure that all devices used to access data (e.g., computers, mobile devices) are password-protected and encrypted where applicable.

2. Secure Data Storage

- All physical records containing personal data must be stored in a locked, secure location.
- Electronic data must be stored on company-approved, encrypted storage systems.
- Avoid storing personal data on portable devices (e.g., USB drives) unless absolutely necessary, and ensure encryption if used.

3. Data Transmission

- When transmitting personal data electronically, always use secure communication channels (e.g., encrypted emails, secure file sharing platforms).
- Avoid sharing personal data via unsecured channels, such as unencrypted email or text messages.
- Ensure that any third parties receiving personal data are compliant with data protection regulations.

4. Data Minimization

- Collect only the data necessary for the specific purpose.
- Avoid keeping personal data for longer than necessary and delete or anonymize data that is no longer required for business purposes.

5. Confidentiality and Integrity

- Maintain the confidentiality of all personal data and do not share it with unauthorized individuals.
- Ensure that personal data is accurate and up to date, correcting any inaccuracies promptly.

6. Training and Awareness

- All employees must undergo regular data protection training to stay informed about best practices, security risks, and legal obligations.
- Stay updated on changes to DCL's Data Protection and Privacy Policy, as well as any relevant laws or regulations.

7. Reporting and Compliance

- Immediately report any suspected data breaches or security issues to the Data Protection Officer (DPO) or supervisor.
- Cooperate with investigations and audits related to data protection compliance.

By adhering to these guidelines, employees would help protect the privacy and security of personal data, ensuring that the company complies with relevant data protection laws and maintains the trust of its clients and stakeholders.

Reviewed by: _____
Signature _____
Name: _____
Date: _____

Approved by: _____
Signature _____
Name: _____

Date: _____