**Brightstar Integral Technology Solution Limited**

**DATA PRIVACY POLICY**

**Document Control**

|  |  |
| --- | --- |
| **Date Created** |  |
| **Document Author** |  |
| **Document Owner** |  |
| **Date Reviewed** |  |
| **Next Review Date** |  |
| **Document Classification** |   |
| **Retention Period** |   |

**Version and Update History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Summary of changes |
| Draft Version1.0 |  |  |   Initial Review |
|  |  |  |  |
|  |  |  |  |

**Approval List**

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Position | Signature | Date |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of Contents**

[1 Introduction 4](#_Toc136614120)

[1.1 Purpose 4](#_Toc136614121)

[1.2 Scope 5](#_Toc136614122)

[1.3 Accountability 5](#_Toc136614123)

[2 Policy Statements 6](#_Toc136614124)

[2.1 Personal Data Processing Principles 9](#_Toc136614125)

[**2.1.1** **Lawfulness, Fairness, and Transparency** 10](#_Toc136614126)

[**2.1.2** **Purpose Limitation** 11](#_Toc136614127)

[**2.1.3** **Data Minimization** 11](#_Toc136614128)

[**2.1.4** **Accuracy** 11](#_Toc136614129)

[**2.1.5** **Storage Limitation** 12](#_Toc136614130)

[**2.1.6** **Security, Integrity, and Confidentiality** 12](#_Toc136614131)

[2.2 Transfers to Foreign Countries 13](#_Toc136614132)

[2.3 Data Subject Rights and Requests 13](#_Toc136614133)

[2.4 Direct Marketing 14](#_Toc136614134)

[2.5 Reporting Personal Data Breaches 14](#_Toc136614135)

[2.6 Data Privacy Guidelines and Data Classification 15](#_Toc136614136)

[3 Responsibilities 17](#_Toc136614137)

[3.1 Brightstar’s Responsibilities 17](#_Toc136614138)

[3.2 Data Protection Office/Manager’s Responsibilities 17](#_Toc136614139)

[3.3 Staff’s Responsibilities 17](#_Toc136614140)

[3.4 Third-Party Data Processors 18](#_Toc136614141)

[3.5 Contractors, Short-Term and Voluntary Staff 18](#_Toc136614142)

[3.6 Changes made to Policy 19](#_Toc136614143)

[4 Violation 19](#_Toc136614144)

# Introduction

## Purpose

The purpose of this policy is to ensure data protection and privacy as required by contractual clauses with Brightstar Integral Technology Solution Limited’s (‘Brightstar’ or ‘Brightstar Tech’) staff, customers, vendors and other third parties as well as to establish standards of compliance with global and domestic data privacy laws.

Brightstar Integral Technology Solution Limited obtains, uses, stores, and otherwise processes personal data relating to current staff and clients, potential staff and clients, former staff and clients, contractors, website users and contacts, collectively referred to in this policy as data subjects. When processing personal data, Brightstar is obliged to fulfil individuals’ reasonable expectations of privacy by complying with the Nigeria Data Protection Regulation (NDPR) and other relevant data protection legislation (data protection law).

This policy seeks to ensure that we:

1. are clear about how personal data must be processed and Brightstar’s expectations for all those who process personal data on its behalf.
2. comply with the data protection law and with good practice.
3. protect Brightstar’s reputation by ensuring the personal data entrusted to us is processed in accordance with data subjects’ rights.
4. protect Brightstar from risks of personal data breaches and other breaches of data protection law.

## Scope

This policy applies to all personal data we process regardless of the location where that personal data is stored (e.g., on an employee’s own device) and regardless of the data subject. All staff and others processing personal data on Brightstar’s behalf must read it. Failure to comply with this policy may result in disciplinary action as highlighted in the violation section.

All are responsible for ensuring that all Brightstar staff within their area of responsibility comply with this policy and should implement appropriate practices, processes, controls, and training to ensure compliance.

Furthermore, Brightstar Integral Technology Solutions Limited takes its responsibilities with regards to the management of the requirements of the Nigeria Data Protection Regulation very seriously. This policy sets out how Brightstar Tech manages those responsibilities.

The Data Protection Office within the IT department are responsible for overseeing this policy. Brightstar’s Data Protection Office can be reached at dataprotection@brightstar.ng

## Accountability

Brightstar Integral Technology Solution Limited must implement appropriate technical and organizational measures in an effective manner to ensure compliance with data protection principles. Brightstar is responsible for, and must be able to demonstrate compliance with, the data protection principles.

We must therefore apply adequate resources and controls to ensure and to document NDPR compliance including:

1. appointing a suitably qualified Data Protection Officer/Manager (DPO/DPM).

2. implementing Privacy by Design when processing personal data and completing a Data Protection Impact Assessment (DPIA) where processing presents a high risk to the privacy of data subjects.

3. integrating data protection into our policies and procedures, in the way personal data is handled by us and by producing required documentation such as Privacy Notices, Records of Processing and records of Personal Data Breaches.

4. training staff on compliance with Data Protection Law and keeping a record accordingly and,

5. regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

# Policy Statements

* Brightstar Integral Technology Solution Limited shall exercise legal ownership of the contents of all files stored on its computer and network systems as well as all messages transmitted via these systems.
* Brightstar Integral Technology Solution Limited reserves the right to access information stored on any computer system connected to the corporate network without prior notice.
* Brightstar Integral Technology Solution Limited shall ensure that all user’s files on its workstations would be backed-up at periodic intervals.
* Data must be classified into different levels of sensitivity classifications with appropriate handling requirements in line with the information classification framework of Brightstar Integral Technology Solution Limited. This standard data sensitivity classification system must be used throughout Brightstar Integral Technology Solution Limited.
* Brightstar Integral Technology Solution Limited’s entire internal information must be protected from disclosure to third parties.
* The Human Resources department must ensure that all employees are fully aware of their legal and corporate responsibilities concerning the inappropriate sharing and releasing of information both internally within Brightstar Integral Technology Solution Limited and to external parties.
* To facilitate the above, the Human Resources department must ensure that the Oath of Secrecy and Confidentiality Agreements are signed by all employees.
* Prior to sending information to third parties, not only must the intended recipient be authorized to receive such information, but the procedures and information security measures adopted by the third party must be seen to continue to assure the confidentiality and integrity of the information.
* Data must be protected against unauthorized access, or accidental changes and may only be deleted with the appropriate authorization.
* Staff in custody of Brightstar Integral Technology Solution Limited’s sensitive information must take appropriate steps to ensure that these materials are not available to unauthorized persons.
* Confidential information must only be disclosed after express authorization has been obtained from the Data Owners or a legal/regulatory requirement in line with Brightstar Integral Technology Solution Limited’s policies. Users permitted to access such information are not permitted to disclose them to others.
* If sensitive information is to be stored on the hard disk drive or other internal components of a personal computer, it must be protected appropriately.
* Information classified as confidential must never be sent to a network printer without there being an authorized person to safeguard its confidentiality during and after printing.
* When sensitive information is written to a magnetic disk, or other storage media, the media must be suitably marked with the highest relevant sensitivity classification. If the marking constitutes an exposure, then such tapes must be kept in secured compartments without marking. When not in use, this media must be stored in locked safes.
* An explicit statement describing exactly what information is restricted and how this information may be used must accompany all disclosures of confidential Brightstar information to third parties.
* Brightstar Tech employees are prohibited from disclosing to anyone outside of Brightstar Integral Technology Solution Limited, the nature of client projects, client business and marketing strategies, or customer business relationships.
* Permission to disclose any internal Brightstar Tech information to the news media or other third parties must be obtained from the Communications Team for this prior to release.
* Staff must not sign confidentiality agreements provided by third parties without the advance authorization of the Legal unit designated to handle intellectual property matters.
* Persons other than those specifically invited must not attend meetings where confidential information will be discussed.
* If confidential information is released verbally at a meeting or related presentation, the speaker must clearly communicate the sensitivity of the information and the need for discretion on the part of the audience. Visual aids such as slides, and overhead transparencies must also include the appropriate confidentiality markings.
* When sensitive information has been recorded on black boards or white boards, it must be definitively erased (with water or special cleaning fluids) before the authorized recipients of this information leave the area.
* Unauthorized access to private user files and folders on Brightstar’s network and computer systems is prohibited.
* Never lend to others a personal computer, handheld computer, transportable computer, personal digital assistant, smart phone, or any other computer that you use for business activities if the machine contains sensitive information.
* Employees must lock all sensitive file cabinets and must provide a backup copy of the key(s) to their department manager.
* The internal system addresses, configurations, and related system design information for Brightstar Integral Technology Solution Limited’s networked computer systems must be restricted such that both systems and users outside Brightstar Integral Technology Solution Limited’s internal network cannot access this information.
* Personal data must not be retained longer than required.
* Regulatory requirements and laws of Nigeria shall take precedence over any standard, law, rules, directive, or framework if the requirements conflict with our legal and regulatory requirements. Generally, we would adopt the stricter security rule, provided it does not violate security requirements in the country of our operations.

## Personal Data Processing Principles

When you process personal data, you should be guided by the following principles, which are set out in the NDPR. Brightstar Tech is responsible for, and must be able to demonstrate compliance with, the data protection principles listed below:

Those principles require personal data to be:

1. processed lawfully, fairly and in a transparent manner (**Lawfulness, Fairness, and Transparency**).
2. collected only for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes (**Purpose Limitation**).
3. adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed (**Data Minimization**).
4. accurate and where necessary kept up to date (**Accuracy**).
5. not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data is processed (**Storage Limitation**).
6. processed in a manner that ensures its security, using appropriate technical and organizational measures to protect against unauthorized or unlawful processing and against accidental loss, destruction, or damage (**Confidentiality, Integrity, and Availability**).

### **Lawfulness, Fairness, and Transparency**

**Lawfulness and Fairness**

In order to collect and process personal data for any specific purpose, Brightstar Tech must always have a lawful basis for doing so. Without a lawful basis for processing, such processing will be unlawful and unfair and may also have an adverse impact on the affected data subjects.

Processing personal data will only be lawful, where at least one of the following lawful bases applies:

1. The data subject has given their **consent** for one or more specific purposes.

2. The processing is necessary for the **performance of a contract** to which the data subject is a party.

3. To comply with Brightstar’s **legal obligations**.

4. To protect the **vital interests** of the data subject or another person (this will equate to a situation where the processing is necessary to protect the individual’s life)

5. To perform tasks carried out in the **public interest** or the exercise of official authority.

6. To pursue Brightstar’s **legitimate interests** where those interests are not outweighed by the interests and rights of data subjects (only available to Brightstar Tech in some circumstances)

**Transparency**

The concept of transparency runs throughout the NDPR and requires Brightstar Tech to ensure that any information provided by Brightstar to data subjects about how their personal data will be processed is concise, easily accessible, easy to understand and written in plain language. Where Brightstar Integral Technology Solutions Limited has not been transparent about how it processes personal data, this will call the lawfulness and fairness of the processing into question.

### **Purpose Limitation**

Brightstar Integral Technology Solutions Limited must only collect and process personal data for specified, explicit and legitimate purposes that have been communicated to data subjects beforethe personal data was collected.

Brightstar Tech must ensure that it does not process any personal data obtained for one or more specific purposes for a new purpose that is not compatible with the original purpose. Where Brightstar Tech intends to do so, it must inform the data subjects before using their personal data for the new purpose and, where the lawful basis relied upon for the original purpose was consent, obtain such consent again.

### **Data Minimization**

The personal data that Brightstar collects, and processes must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is to be processed.

You must only process personal data when necessary for the performance of your duties and tasks and not for any other purposes. Accessing personal data that you are not authorized to access, or that you have no reason to access, may result in disciplinary action and in certain circumstances, may constitute a criminal offence.

You may only collect personal data as required for the performance of your duties and tasks and should not ask a data subject to provide more personal data than is strictly necessary for the intended purposes.

You must ensure that when personal data are no longer needed for the specific purposes for which they were collected, such personal data are deleted, destroyed, or anonymized.

**You must observe and comply with Brightstar’s Data Retention and Archival Policy.**

### **Accuracy**

The personal data that Brightstar collects, and processes must be accurate and, where necessary, kept up-to-date and must be corrected or deleted without delay when Brightstar discovers, or is notified, that the data is inaccurate.

**You must ensure that you update all relevant records if you become aware that any personal data is inaccurate. Where appropriate, any inaccurate or out-of-date records should be deleted or destroyed.**

### **Storage Limitation**

The personal data that Brightstar Tech collects, and processes must not be kept in a form that identifies a data subject for longer than is necessary in relation to the purposes for which it was collected (except to comply with any legal, accounting or reporting requirements).

Storing personal data for longer than necessary may increase the severity of a data breach and may also lead to increased costs associated with such storage.

### **Security, Integrity, and Confidentiality**

**Security of personal data**

The personal data that Brightstar Tech collects, and processes must be secured by appropriate technical and organizational measures against accidental loss, destruction, or damage, and against unauthorized or unlawful processing.

Brightstar Tech will develop, implement, and maintain appropriate technical and organizational measures for the processing of personal data considering the:

* nature, scope, context, and purposes for such processing
* volume of personal data processed
* likelihood and severity of the risks of such processing to the rights of data subjects

Brightstar Integral Technology Solutions Limited will regularly evaluate and test the effectiveness of such measures to ensure that they are adequate and effective.

You are responsible for ensuring the security of the personal data processed by you in the performance of your duties and tasks. You must ensure that you follow all procedures that Brightstar has put in place to maintain the security of personal data from collection to destruction.

You must ensure that the **confidentiality, integrity**, and **availability** of personal data are always maintained:

• **Confidentiality:** means that only people who need to know and are authorized to process any personal data can access it

• **Integrity:** means that personal data must be accurate and suitable for the intended purposes

• **Availability:** means that those who need to access the personal data for authorized purposes can do so

**You must not attempt to circumvent any administrative, physical, or technical measures Brightstar has implemented as doing so may result in disciplinary action and in certain circumstances, may constitute a criminal offence.**

## Transfers to Foreign Countries

Where Personal Data is to be transferred to a country outside Nigeria, Brightstar shall put adequate measures in place to ensure the security of such Personal Data. Brightstar Tech shall, among other things, conduct a detailed assessment of whether the said country is on the Nigeria Data Protection Bureau (NDPB) Whitelist of Countries with adequate data protection laws.

**Transfer of Personal Data out of Nigeria would be in accordance with the provisions of the NDPR and Brightstar’s Procedure for International Transfers of Personal Data.**

## Data Subject Rights and Requests

Subject to applicable laws such as the Nigeria Data Protection Regulation, Data subjects can exercise the following rights regarding their data:

* To request a copy of the personal data processed on their behalf
* To request that we correct their personal data
* To request us to delete their personal data, for example if we no longer have a valid reason to process it
* To object to how we process their personal data
* To restrict how the data subject’s personal data is processed in certain cases, such as when the accuracy of the personal data is contested
* To request a copy of the personal data that we hold and process about the data subject in a machine-readable format.

## Direct Marketing

In addition to Brightstar’s obligations under the NDPR, it is also subject to more specific rules in relation to direct marketing by email, fax, SMS, or telephone.

Brightstar Tech must ensure that it has appropriate consent from individuals to send them direct marketing communications, and that when a data subject exercises their right to object to direct marketing, it has honored such requests promptly.

**You must ensure that you understand or consult with the Data Protection Officer (DPO) on Brightstar’s legal obligations in relation to direct marketing before embarking upon any direct marketing campaign.**

## Reporting Personal Data Breaches

Brightstar Tech has a duty of self-reporting of Personal Data breaches to NDPB within 72 hours of becoming aware of such breach.

Furthermore, Brightstar will notify data subjects of the personal data breach where the data breach will likely result in high risks to the freedom and rights of the data subject.

If you know or suspect that a personal data breach has occurred, you must contact the **Data Protection Officer** immediately to report it and obtain advice and take all appropriate steps to preserve evidence relating to the breach.

**You must ensure that you observe and comply with Brightstar Integral Technology Solution Limited’s Personal Data Breach Notification Procedure.**

## Data Privacy Guidelines and Data Classification

**Guidelines**

* Third parties may be given access to Brightstar Integral Technology Solution Limited’s internal information only when a demonstrable need-to-know exists, and when such a disclosure has been expressly authorized by the Data Owners and or a legal/regulatory requirement in line with Brightstar Integral Technology Solution Limited’s policies.
* Protection for sensitive information may be by either a password access control package or encryption.
* As a rule, information security policies and procedures should be revealed to only Brightstar staff and select outsiders (such as auditors) who have a legitimate business need for this information.
* Although, certain marketing information is customarily disclosed to outsiders, they should never be disclosed to competitors. Likewise, marketing strategies, marketing plans, market share status, and other marketing information should never be shared with competitors.
* System administrators are authorized to examine private user files to handle emergencies such as virus infestations and system crashes. Whenever user files are to be examined in this manner, the involved user(s) should be notified. After the problem has been resolved, all copies of such files made by the administrator should be promptly destroyed.
* In order to maintain security and to prevent processing in infringement of regulation, (as a data controller or processor) we would evaluate the risks inherent in processing collected personal identifiable data and implement measures to mitigate those risks, this could be by encryption and restricted access.
* Brightstar Integral Technology Solution Limited must notify staff as promptly as possible, within a period not exceeding two (2) hours, of the occurrence of an incident or from a determination that a cyber-security incident has occurred, that is either of the following:
* Cyber-security incident that may prevent Brightstar from continuing its normal operations for client-facing transactions, and
* Cyber-security events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of Brightstar Tech.
* A Data Protection Officer shall be designated.
* Highlights of the privacy policy may be published on Brightstar Integral Technology Solutions Limited’s corporate website.

**Data Classification**

Brightstar’s data classification shall be as follows:

1. **Confidential**

This classification refers to highly sensitive internal documents, which could seriously damage Brightstar Integral Technology Solution Limited if lost or made public. Information classified as Confidential has very restricted distribution and must be always protected. Security at this level is the highest possible. Examples include **impending mergers or acquisitions, corporate plans, marketing strategies, designs, designs, or employee and customer personal information**.

1. **Internal Use**

This classification refers to Information not approved for general circulation outside the organization where its disclosure would inconvenience the organization or management but is unlikely to result in financial loss or serious damage to credibility. Examples **include internal memos, minutes of meetings, internal project reports**. Security at this level is controlled but normal.

1. **Public**

This classification applies to all information meant for public use. Their disclosure will not adversely impact Brightstar Integral Technology Solution Limited, its employees, stakeholders, business partners, and/or customers. Examples include newsletters, annual reports, published financial statements, etc. Security at this level is minimal.

# Responsibilities

## Brightstar’s Responsibilities

As the Data Controller, Brightstar Tech is responsible for establishing policies and procedures in order to comply with data protection laws.

## Data Protection Office/Manager’s Responsibilities

The DPO is responsible for:

(a) advising Brightstar Tech and its staff of its obligations under NDPR.

(b) monitoring compliance with this regulation and other relevant data protection laws, Brightstar’s policies with respect to this and monitoring training and audit activities related to NDPR compliance.

(c) providing advice where requested on data protection impact assessments.

(d) cooperating with and acting as the contact point for the Supervisory Authority (National Information Technology Development Agency).

(e) the data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, considering the nature, scope, context, and purposes of processing.

## Staff’s Responsibilities

Staff members who process personal data about clients, staff, or any other individual must comply with the requirements of this policy. Staff members must ensure that:

(a) all personal data is kept securely

(b) no personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorized third party

(c) personal data is kept in accordance with Brightstar’s retention schedule

(d) any queries regarding data protection, including subject access requests and complaints, are promptly directed to the Data Protection Officer

(e) any data protection breaches are swiftly brought to the attention of the Data Protection Officer and that they support in resolving breaches

(f) where there is uncertainty around a data protection matter, advice is sought from the Data Protection Officer.

## Third-Party Data Processors

Where external companies are used to process personal data on behalf of Brightstar tech, responsibility for the security and appropriate use of that data remains with Brightstar.

Where a third-party data processor is used:

(a) a data processor must be chosen which provides sufficient guarantees about its security measures to protect the processing of personal data

(b) reasonable steps must be taken that such security measures are in place

(c) a written contract establishing what personal data will be processed and for what purpose must be set out

(d) a data processing agreement, available from the Information Technology, Legal, Human Resources, Customer Experience, Operations and Compliance teams, must be signed by both parties.

For further guidance about the use of third-party data processors please contact the Information Technology, Legal and Compliance teams.

## Contractors, Short-Term and Voluntary Staff

Brightstar is responsible for the use of personal data by anyone working on its behalf. Managers who employ contractors, short term or voluntary staff must ensure that they are appropriately vetted for the data they will be processing. In addition, managers should ensure that:

(a) any personal data collected or processed in the course of work undertaken for Brightstar Tech is kept securely and confidentially.

(b) all personal data is returned to Brightstar Tech on completion of the work, including any copies that may have been made. Alternatively, that the data is securely destroyed, and Brightstar receives notification in this regard from the contractor or short term / voluntary member of staff.

(c) Brightstar Tech receives prior notification of any disclosure of personal data to any other organization or any person who is not a direct employee of the contractor.

(d) any personal data made available by Brightstar, or collected in the course of the work, is neither stored nor processed outside Nigeria unless a written consent to do so has been received from Brightstar.

(e) all practical and reasonable steps are taken to ensure that contractors, short term, or voluntary staff do not have access to any personal data beyond what is essential for the work to be carried out properly.

## Changes made to Policy

Updates may be made to this policy from time to time to reflect changes in our privacy practices and ensure compliance with the various the Data Privacy Regulation set and monitored by the Nigeria Data Protection Bureau (NDPB). The revised policy will be reposted on our website and will be shared to all stakeholders before becoming effective.

# Violation

Brightstar Integral Technology Solution Limited will regard the violation of this policy by employees or business partners as a disciplinary offense, which could result in a disciplinary sanction up to and including dismissal or termination of employment and discontinuation of business relations. In addition, if laws are violated, employees or the company may be subject to criminal penalties (fines or jail time) or civil sanctions (damage awards or fines). Brightstar Tech could also be restricted or prohibited in processing information in the manner necessary to conduct normal business operations.