

NOVA BANK

MARCH 2024

DATA PROTECTION
POLICY

Contents

1.0 Purpose.....	4
1.1 Notice of Compliance.....	4
2.0 Scope.....	4
3.0 Appointment of DPCO.....	5
4.0 Responsibilities and Definitions.....	5
5.0 Processing of Personal Data.....	9
6.0 Special Category (Sensitive) Data.....	10
7.0 Categories of Data Processed by Nova.....	11
8.0 Access Rights.....	11
9.0 Data Privacy Impact Assessment.....	12
10.0 Remediation for Data Breach.....	12
11.0 CCTV.....	12
12.0 Documentation.....	13
13.0 Appendices.....	13

1.0 Purpose

This policy contains security measures for developing, administering and managing systems, including operating systems, databases, applications and network devices and data. The purpose of this policy is to provide a comprehensive set of security requirements to ensure protection of NOVA's customers/clients and third-party confidential information entrusted to NOVA or to which access is otherwise available.

This policy also provides those security measures that are applicable to end users and describes behaviours that are required to maintain those measures. All NOVA staff, as well as any third parties that require access to NOVA systems (e.g., contractors, regulators, etc.) are end users, and are responsible for compliance. The policy also provides guidelines for the implementation of processes involving data subject sensitive information.

1.1 Notice of Compliance

Security is the responsibility of everyone accessing NOVA systems, NOVA data and data entrusted to NOVA by clients or other third parties. The security measures described herein define the minimum level of security required for NOVA systems and information from the National Information Technology development agency (NITDA) and the central bank of Nigeria (CBN). Non-compliance with the required security measures and behaviours outlined in this policy could pose significant business and legal risk to NOVA and may create a potential for legal actions that could significantly impact NOVA's operations and damage its business assets and reputation. Therefore, compliance with this policy and all other NOVA security-related policies is mandatory and deemed a condition of continuous employment for all NOVA staff. It is also deemed a condition for continuous engagement of the services of third parties (such as outsourcing providers, contractors, regulators, clients, etc.) that access NOVA systems or data. No one is permitted to bypass the security mechanisms provided by NOVA systems or infrastructure for any reason. Failure to comply with this policy will be reported and disciplinary action may be taken.

2.0 Scope

2.1 The General Data Protection Regulations (GDPR) and the Nigerian Data Protection Regulation (NDPR) provide individuals with rights in relation to personal data held/processed by organisations. The regulations also place obligations on organisations to have appropriate technical and organisational measures in place to ensure the integrity and confidentiality of personal information held/processed.

2.2 NOVA holds and processes information about its staff, consultants, customers, contractors and other stakeholders for various purposes including its obligations as a responsible and effective employer, in order to operate payroll and pension services and to comply with its obligations to facilitate effective communication with those stakeholders. To comply with GDPR and NDPR information must be processed lawfully and fairly, collected for specified purposes, stored safely, be

accurate and kept up to date as necessary and not disclosed to any unauthorised person or organisation.

- 2.3 NOVA has a statutory obligation as a Data Controller/Processor to be responsible for and be able to demonstrate compliance with the legislation. All staff can obtain full details of this policy and NOVA's data subjects from the Data Protection Officer (DPO) and from NOVA's intranet.
- 2.4 This policy defines the responsibilities of the NOVA and its employees, contractors and consultants and ensures that all are aware, not only of the requirements of data protection regulation on the NOVA itself, but also their individual responsibilities in this respect. A failure to comply with the provisions of NDPR may render NOVA, or in certain circumstances the individuals involved, including the NOVA Data Protection Officer and the relevant responsible director(s) liable.
- 2.5 This policy must be read in conjunction with its corresponding Nigeria data protection regulations as stipulated by the National Information Technology Development Agency (NITDA).

3.0 Appointment of Data Protection Compliance Organization (DPCO)

The executive management of NOVA through the MD, shall appoint, on an annual basis, a National Information Technology Development Agency (NITDR) approved Data Protection Compliance Organization (DPCO) to carry out audit and file a report with NITDA on or before March 15 of the year.

4.0 Responsibilities and Definitions

- 4.1 The NOVA **Data Protection Officer** is responsible for ensuring that statutory and regulatory obligations with respect to the GDPR and NDPR are adhered to and for the provision of monitoring, training, guidance and advice to ensure policy compliance with data privacy regulations by all NOVA employees, consultants and contractors. They are also the individual to whom all subject access requests and queries concerning personal data should be addressed. The DPO is to communicate with the regulator on all matters as required by regulation and in the event of any breach of personal data, he is to communicate to internal and external stakeholders within the stipulated timelines. Communicating with management and staff on compliance and obligations regarding GDPR and NDPR

4.2 Chief Information Security Officer (CISO)

In the event of a data breach, the CISO is to:

- communicate to the MD/CEO on the nature, scope and gravity of the Personal Data breach.

- lead the Incident Response Team in the breach investigation and assessment.
- he is to recommend the approval of anyone who requests for privilege profile to the Executive Management.
- supervise his team in performing Data Privacy Impact Analysis (DPIA).
- responsible for Data Privacy Awareness Training for staff - both new (at onboarding) and old.

4.3 Chief Information Officer (CIO)

The CIO is to ensure that applications developed in-house complies with the requirements of GDPR and NDPR regulations (e.g. cookie policy requirements, privacy by design, privacy by default etc.). For all application developments, live and test environments should be different and live data should not be used in test environments.

4.4. Employees

NOVA staff members are to comply with NOVA data protection policies and processes. It is their responsibility to participate in data privacy trainings.

4.5 Senior Executive Management/MD/CEO

- Approves the appointment of a DPO.
- Provides enabling environment for the DPO to ensure compliance and treat access and rectification requests.
- The senior management through the MD/CEO is to report data protection compliance status to NOVA Board
- Based on the DPO's recommendation, approves notification to relevant stakeholders in the event of a data breach.

4.6 Board Members

Ensure that senior management is accountable for compliance to NDPR and GDPR requirements.

4.7 **The National Information Technology Development Agency** is the Nigeria's independent authority set up to promote access to official information and to protect personal information.

4.8 **Data Controller** is the person or organisation who determines the purposes for which and the way any personal data are to be processed. In NOVA it is the registered Data Controller.

- 4.9 **Data Processor** is any individual or company who records and/or processes personal data in any form on behalf of NOVA.
- 4.10 **NOVA Directors, Departmental and Functional Heads** are responsible for the promulgation of this policy and any associated guidance within their own business unit.
- 4.11 **NOVA permanent and temporary employees, contractors, consultants and other data users** are responsible for incorporating this policy and its associated documents into their own working practices.
- 4.12 **Data Processing** in relation to this policy means:
- collection, recording, organisation, structuring, storage.
 - carrying out any operation, or set of operations, on the information including:
 - organisation, adaptation or alteration of the information.
 - retrieval, consultation or use of the information.
 - disclosure of the information by transmission, dissemination or otherwise making available.
 - alignment, combination, blocking, erasure or destruction of the information.
- 4.13 **Data Subject** means any individual who is the subject of personal data, an employee, contractor, consultant, stakeholder or third party about whom NOVA holds personal data.
- 4.14 **Personal Data** is defined as data which relate to an identified or identifiable person (data subject). An identifiable person is one who can be identified directly or indirectly. In particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person from those data and other information, which is in the possession of, or is likely to come into the possession of, the data controller and includes expressions of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of that individual.
- 4.15 **Special categories of data** refers to personal data revealing; racial or ethnic origins; political opinions, religious or philosophical beliefs; trade-union membership, genetic data, biometric data, data concerning health.
- 4.16 **Subject Access Request** is a written request from an individual to access any personal data that NOVA holds about him/her. He/She also has the right to request the correction of any such data that is found to be incorrect.

5.0 Processing of Personal Data

5.1 The GDPR and NDPR provide principles to be adhered to in the processing of personal data. This is achieved by NOVA in implementing appropriate rules and procedures. **All** NOVA employees, contractors and consultants are therefore responsible for ensuring that these rules and procedures are followed. The objectives of the rules and procedures are to ensure that the principles will be complied with, and that all personal data is:

- processed lawfully and fairly and in a transparent manner.
- collected for specified, explicit legitimate purposes and not further processed in a manner incompatible with those purposes.
- adequate, relevant and limited to what is necessary in relation to the purposes.
- accurate and where necessary kept up to date.
- kept in a form which permits identification for no longer than is necessary for the specified purpose.
- kept secure subject to appropriate technical and organisational measures against unauthorised or unlawful processing, accidental loss or destruction.

Under the terms of the GDPR and NDPR, processing of data includes any activity to do with the data involved. All employees or other individuals who have access to, or who utilise, personal data, have a responsibility to exercise care in the treatment of that data and to ensure that such information is not disclosed to any unauthorised third party. Examples of personal data could include address lists and contact details as well as individual files. Any processing of such information must be done in accordance with the NOVA rules and procedures.

Additionally, in order to comply with the first principle, at least one of the following conditions must also be met.

- the subject has given his/her explicit consent to the processing (such consent must be recorded).
- the processing is necessary for the performance of a contract with the subject.
- processing is required under a legal obligation.
- processing is necessary to protect the vital interests (essential for the life) of the subject or another person.
- processing is necessary for the performance of a task carried out in the public interest.

- processing is necessary to pursue the legitimate interests of the Data Controller or third parties (unless it could prejudice the interests of the subject or would constitute processing carried out by a public authority in the performance of their tasks).

6.0 Special Category (sensitive) Data

If the personal data is deemed to be sensitive, then additional conditions apply to its processing. Essentially, the explicit consent of the individual will usually have to be obtained before the data is processed unless the data controller can prove the processing is based on one of the following criteria.

- Compliance with employment law and obligations.
- To protect vital interests (essential for the life) of the data subject.
- The data subject has deliberately made the information public.
- To comply with legal obligations (establishing or defending legal rights).
- Processing is necessary for the establishment, exercise or defence of legal claims.
- Processing is necessary for reasons of substantial public interest.
- Occupational medicine, provision of health or social care or treatment.
- Public health.
- Scientific or historical research or statistical purposes.

If you cannot justify the processing and holding of sensitive data, for one of the above reasons you must reconsider whether you should be gathering or holding that data at all. If the data needs to be held you must then obtain the explicit written consent from the data subject to ensure compliance (records of consent must be maintained to cover the entirety of the time the data is held/processed). If you do not have a lawful basis to justify holding/processing this category of data, you must remove the data from your records.

7.0 Categories of data processed by NOVA

Personal data (e.g. name, home address, location data, e-mail address, Account Number, BVN, Social Security Number, Tax Identification Number etc.)

Sensitive data (e.g. religious beliefs, medical data, political opinions etc.)

8.0 Access rights

Data subjects have the right to access personal data that NOVA holds about them. Such a request is called a subject access request (SAR) and the procedure has to be followed to process the request. However, in summary, requests must be.

- processed by the DPO or suitably trained deputy.
- confirmed that the data subjects are who they say they are and have a right of access to the information.
- checked to ensure that any third-party data subject's rights are not overlooked.
- respond to requests without undue delay and in any event within one month of receipt.
- recorded accurately.

It is also possible that NOVA may also receive request from a data subject to erase personal data, rectify inaccurate data, restrict/cease or not begin processing personal data. All such requests or notices must be referred to the DPO and responded to either by:

- agreeing to comply with the request or
- giving the reasons why the request is regarded as unjustified, either wholly or in part.

9.0 Data Privacy Impact Assessments

Data Privacy impact assessments (DPIAs) are a tool that you can use to identify and reduce the privacy risks of projects. This is used to assess the risk to personal data. A DPIA can reduce the risks of harm to individuals through the misuse of their personal information. It can also help you to design more efficient and effective processes for handling personal data.

A DPIA should be carried out whenever a "new" project/process or a change to an existing project/process especially when it affects how personal information is to be handled and it is involving the use of personal information is being considered/initiated, especially if this involves the use of technology or third-party processors e.g. new IT systems or contractors conducting work involving the processing of personal data. The NOVA DPO should be consulted. This should be done at least yearly or when there is a substantial, change relating to personal data as part of the risk assessment function of the Information Security team.

- The focus of the DPIA should be on the Personal Rights of data subjects and the controls around personal data.
- The damage that could arise from the processing of employees and customers personal data.

- The retention and deletion of personal data.
- The availability of the consents of the data subjects.

10.0 Remedies for Data Breach

In the event of data privacy breach relating to a data subject personally identifiable information, the subject has the right to lodge a complaint with the Bank through the Data Protection Officer. NOVA is expected to respond to the Data Breach within 72 hours of receiving information relating to the breach. The DPO has a responsibility to lead investigation and respond to the data subject and remedy the data breach. A data subject can seek compensation from the Bank for a violation of the personal data if the response is not satisfactory. The Bank will not be liable to provide compensation to the data subject if it can be proven that it is not responsible for the event that led to the damage.

11.0 CCTV

NOVA operates a number of CCTV cameras in order to assist with security for its community and property. If any member of staff, consultant or contractor has any queries concerning the operation of these systems, he/she should contact the DPO or the Chief information Officer (CIO) in the absence of the DPO.

12.0 Documentation

NOVA as a controller and processor will always, document its activities on data privacy based on regulatory requirements be it in the form of contracts or records kept by the relevant units.

- Records of subject access requests (Retained for 5 years)
- Records of communications resulting in an action to cease processing personal data (Retained for 5 years)
- CCTV records (Retained for 30 days unless otherwise required for longer as identified by the DPO and the CIO)

13.0 Appendices

There are no appendices associated with this Policy.