THE TOURIST COMPANY OF NIGERIA PLC

Data Protection Policy

Federal Palace
HOTEL AND CASINO
★★★★★

March 2021

Document Control Information

Document Details

Document Title	**Data Protection Policy**
Document Owner	Ralf Schröder

Document Approval

Document Approvers	David Kliegl
Approval Date	10th March 2021
Live Date	11th March 2021

Document Revision History

Version	Date	Updated By	Change Detail
1.0	1st March 2021	Ralf Schröder	Original
2.0	12th April 2022	Ralf Schröder	8.12. Incident response added to the policy

Table of Contents

Federal Palace

1.0 Introduction

The Tourist Company of Nigeria Plc. (TCN) trading as Federal Palace Hotel and Casino, operating within the hospitality and tourism industry needs to gather and process certain information about individuals with whom it has a relationship for various purposes such as, but not limited to the recruitment and payment of staff, relationship management with Members, investors and guests. In light of the emerging data regulatory environment which requires higher transparency and accountability in how companies manage and use personal data, the Company must ensure that its business operations align with global best practices on the protection of rights and privacy of individuals.

2.0 Policy

The Data Protection Policy (the Policy) is a formal acknowledgement that the Company is committed to the protection of rights and privacy of individuals, in accordance with the Nigeria Data Protection Regulation, 2019 (the Regulation).

3.0 Description

The Policy describes how the Company shall collect, handle and store the personal data of individuals to meet the data protection standards.

4.0 Definitions

- **Consent** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her
- **Data** means characters, symbols and binary on which operations are performed by a computer which may be stored or transmitted in the form of electronic signals is stored in any format or any device
- **Database** means a collection of data organised in a manner that allows access, retrieval, deletion and procession of that data; it includes but is not limited to structured, unstructured, cached and file system type databases
- **Data Administrator** means a person or organisation that processes data
- **Data Controller** means a person who either alone, jointly with other persons or in common with other persons or as a statutory body, determines the purposes for and how personal data is processed or is to be processed

Federal Palace

- **Data Portability** means the ability for data to be transferred easily from one IT system or computer to another through a safe and secure means in a standard format
- **Nigeria Information Technology Development Agency** - NITDA
- **Data Protection Compliance Organisation (DPCO)** means any entity duly licensed by NITDA for training, auditing, consulting and rendering services and products for compliance with this Regulation or any foreign Data Protection law or regulation having effect in Nigeria
- **Data Subject** means an identifiable person; one who can be identified directly or indirectly, in particular by reference to an identification number or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity
- **Party** means directors, shareholders, servants and privies of a contracting party
- **Personal Data** means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifiers such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM and others
- **Processing** means any operation or set of operations that are performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
- **Personal Data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed
- **Record** means public record and reports in credible news media
- **Sensitive Personal Data** means data relating to religious or other beliefs, sexual tendencies, health, race, ethnicity, political views, trades union membership, criminal records or any other sensitive personal information

5.0 Purpose

The purpose of this policy is to:

- Protect the Company from the risks of a data breach
- Disclose how TCN stores and processes individuals' data
- Protect the rights of staff, members and stakeholders
- Comply with the Regulation and follow international best practices

6.0 Nigeria Data Protection Regulation

The Regulation, which came into force on January 25, 2019, regulates the gathering, storing and processing of personal data (regardless of whether data is stored electronically, on paper or other materials), and protects the rights and privacy of all living individuals (including children). The Regulation applies to natural persons residing in Nigeria or residing outside Nigeria but of Nigerian descent.

7.0 Applicability

TCN will be the data controller under the terms of the Regulation – this means it is ultimately responsible for controlling the use and processing of personal data. TCN shall appoint a Data Protection Officer (DPO) to ensure adherence to this Regulation, relevant data privacy statements and data protection directives of the Company.

8.0 Governing Principles of Data Protection

The Regulation mandates every data controller to process any personal data following the governing principles of data protection. To comply with the obligations, TCN undertakes to adhere to the following principles.

8.1. Data Processing

The following statement shall guide compliance with the Regulation on data processing. TCN shall:

- Collect and process personal data following specific, legitimate and lawful purpose consented to by the data subject
- Take reasonable steps to ensure that any personal data is accurate
- Store personal data about an individual that is sufficient for the purpose it is holding it for concerning that individual
- Store individuals' data only for the period within which it is reasonably needed

- Secure personal data against all foreseeable hazards, breaches such as theft, cyberattack, viral attack, dissemination, manipulations of any kind, damage by rain, fire or exposure to other natural elements
- Exercise duty of care of personal data in its possession
- Be accountable for its acts and omissions in respect of data processing and following the Regulation

8.2. Lawful Processing

The Company shall process the personal data of individuals if at least one (1) of the following applies:

- The data subject has given consent to the processing of his or her data for one or more specific purposes
- Processing is necessary for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject before entering into a contract
- Processing is necessary for compliance with a legal obligation to which TCN is subject
- Processing is necessary to protect the vital interests of the data subject or another natural person
- Processing is necessary for the performance of a task carried out in the public interest or the exercise of official public mandate vested in TCN

8.3. Procuring Consent

To fulfil the requirement of the Regulation, personal data will be processed following the rights of the data subject. The Company's business operations will be guided by the following statements:

- TCN shall not obtain personal data except the specific purpose of collection is made to the data subject
- The Company shall ensure that consent of the data subject has been obtained without fraud, coercion or undue influence
- The Company shall ensure that the data subject has consented to the processing of his or her data and the legal capacity to give consent, where processing is based on consent
- The Company shall request for consent in a manner which is distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language, where the data subject's consent is given in the context of a written declaration

- The Company shall inform the data subject his/her right and the ease to withdraw his/her consent at any time
- When TCN is assessing whether consent is freely given, the Company shall take utmost account of whether the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary or excessive for the performance of the contract
- The Company shall request for consent of the data subject where data may be transferred to a third party for any reason

8.4. Due Diligence and Prohibition of Improper Motives

To align with these requirements, the Company shall:

- Not seek consent that may engender direct or indirect propagation of atrocities, hate, child rights violation, criminal acts and anti-social conducts
- Take reasonable measures to ensure that a party to any data processing contract does not have a record of violating the Regulation and such party is accountable to NITDA or a reputable regulatory authority for data protection within or outside Nigeria

8.5. Privacy Policy

The Company shall display a simple and conspicuous privacy policy that the class of data subjects being targeted can understand, irrespective of the medium through which such personal data are being collected or processed. TCN's privacy policy shall contain the following:

- Constitution of data subjects' consent
- Description of collectable personal information
- Purpose of collection of personal data
- Technical methods used to collect and store personal information, cookies, web tokens, etc.
- Access, if any, of third parties to personal data and purpose of access
- A highlight of the principles governing data processing
- Available remedies in the event of a violation of the privacy policy
- The time frame for remedy
- Any limitation clause provided that the limitation clause does not exonerate TCN from breaches of the Regulation

8.6. Data Security

TCN recognises the importance of protecting data from unauthorised access and data corruption and the Company shall:

- Develop security measures including but not limited to protecting systems from hackers
- Set up firewalls and protect email systems
- Store data securely with access to specifically authorised individuals
- Employ data encryption technologies
- Develop an organisational policy for handling personal data and other sensitive or confidential data
- Continuously build capacity for all staff

8.7. Third-Party Data Processing Contracts

To ensure compliance with the Regulation, being a data controller, the Company shall:

- Ensure that a written contract is signed by a third party that will process the personal data of individuals
- Ensure that such third party that will process the data obtained from data subjects complies with the Regulation

8.8. Objections by the Data Subject

The Company acknowledges that individuals have the right to object to the processing of their data, as such the Company shall only process personal data following data subjects' rights as listed below:

- Option to object to the processing of personal data relating to the data subject which TCN intends to process for marketing
- Option to be expressly and manifestly offered the mechanism for objection to any form of data processing free of charge

8.9. Transfer to a Foreign Country

The Company shall comply with the Regulation and any transfer of personal data which is undergoing processing or is intended for processing after transfer to a foreign country or an international organisation shall take place subject to the provisions of the Regulation.

8.10. Exceptions in Respect of Transfer to a Foreign Country

In the absence of any decision made by NITDA or Honourable Attorney General of the Federation (HAGF) on the transfer of personal data to a foreign country, TCN shall initiate the transfer or set of transfers of personal data to such foreign country or an international organisation only when:

- The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards and that there are no alternatives
- The transfer is necessary for the performance of a contract between the data subject and TCN or the implementation of pre-contractual measures taken at the data subject's request
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between TCN and another natural or legal person
- The transfer is necessary for important reasons of public interest
- The transfer is necessary for the establishment, exercise or defence of legal claims
- The transfer is necessary to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent

TCN, in compliance with the Regulation, shall explicitly communicate through clear warnings of the specific principle(s) of data protection that are likely to be violated in the event of a transfer to a third country.

8.11. Rights of Data Subjects

To comply with this section under the Regulation, TCN shall:

- Take appropriate measures to provide any information relating to processing, to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child
- Provide such information in writing, or by other means, including, where appropriate, by electronic means
- Provide any information relating to the processing of data obtained from the data subject orally, at the request of the data subject, provided that the identity of the data subject is proven by other means
- Inform the data subject without delay and at least within one (1) month of receipt of a request relating to the processing of his/her data, the reasons for not providing the information and the possibility of lodging a complaint with the supervisory authority

- Provide information, any form of communication or any actions taken to a data subject free of charge
- Charge data subject if a request for his/her data is manifestly unfounded or excessive, in particular, because of his/her repetitive character. The charge shall be a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested
- Write a letter to the data subject stating "refusal act" on the request and copy NITDA on every occasion through a dedicated channel which shall be provided for such purpose, provided that such request is excessive
- Bear the burden of demonstrating the manifestly unfounded or excessive character of the request
- Request for provision of additional information necessary to confirm the identity of the data subject where the Company has reasonable doubts concerning the identity of the requestor
- Provide the information in combination with standardised icons to give in an easily visible, intelligible and legible manner, a meaningful overview of the intended processing and machine-readable format when presented electronically
- Provide the data subject with all of the following information, before collecting personal data:
    - The identity and the contact details of TCN
    - The contact details of the Data Protection Officer
    - The purposes of the processing for which the personal data are intended as well as the legal basis for the processing
    - The legitimate interests pursued by TCN or by a third party
    - The recipients or categories of recipients of the personal data, if any
    - Where applicable, the fact that TCN intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by NITDA
    - The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
    - The existence of the right to request from TCN, access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to the processing as well as the right to data portability
    - The existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal
    - The right to complain to a relevant authority
    - Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and the possible consequences of failure to provide

such data

- The existence of automated decision-making, including profiling and, at least, in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject
- Where TCN intends to further process the personal data for a purpose other than that for which the personal data were collected, the Company shall provide the data subject before that further processing with information on that other purpose and with any relevant further information
- Where applicable, that the Company intends to transfer personal data to a recipient in a foreign country or international organisation and the existence or absence of an adequacy decision by NITDA

- Inform the data subject of the appropriate safeguards for data protection in the foreign country
- Rectify, without undue delay, inaccurate personal data concerning data subjects per their requests
- Acknowledge the right of data subjects to have their incomplete data completed, including by providing a supplementary statement
- Delete personal data without delay, upon request of the data subject
- Delete personal data where one of the following grounds applies:
  - The personal data are no longer necessary concerning the purposes for which they were collected or processed
  - The data subject withdraws consent on which the processing is based
  - The data subject objects to the processing and there are no overriding legitimate grounds for the processing
  - The personal data have been unlawfully processed
  - The personal data have to be erased for compliance with a legal obligation in Nigeria
- Take all reasonable steps to delete all the personal data made public and inform other companies processing the personal data of the data subject request
- Acknowledge data subjects' rights to obtain restriction of processing their data where one of the following applies:
  - The accuracy of the personal data is contested by the data subject for a period enabling TCN to verify the accuracy of the personal data
  - The processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead
  - TCN no longer needs the personal data for the processing but they are required by the data subject for the establishment, exercise or defence of legal claims
  - The data subject has objected to processing pending the verification to confirm whether the legitimate grounds of TCN override those of the data subject

Federal Palace

- Process personal data with the data subject consent, where processing has been restricted
- Communicate any rectification or erasure of personal data or restriction to each recipient to whom the personal data has been disclosed, unless this proves impossible or involves disproportionate effort
- Provide personal data concerning data subjects, in a structured manner, commonly used and machine-readable format to such data subjects
- Not hinder the data subject from transmitting those data in its database to another company where the processing is based on consent, on a contract and processing is carried out by automated means
- Execute data subjects' requests on the transmission of their data to another company, where technically feasible

8.12. Incident response

Reporting of personal data breaches shall be reported to NITDA within 72 hours and affected data subjects within 7 days from the time of the incident.

Notification to NITDA will include:

- A description of the circumstances of the loss or unauthorized access or disclosure;
- The date or time during which the loss or unauthorized access or disclosure occurred
- A description of the personal information involved in the loss or unauthorized access or disclosure
- An assessment of the risk of harm to individuals as a result of the loss or unauthorized access or disclosure
- An estimate of the number of individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure
- A description of any steps the organization has taken to reduce the risk of harm to individuals
- A description of any steps the organization has taken to notify individuals of the loss or unauthorized access or disclosure, and
- The name and contact information for a person who can answer, on behalf of the organization, the Agency's questions about the loss of unauthorized access or disclosure

9.0 Roles and Responsibilities

In compliance with the Regulation, the Company has identified key stakeholders and their responsibilities to drive the operationalisation of the Policy and implementation of necessary data protection controls.

9.1. Board

- Set the tone at the top on data protection
- Ultimately responsible for ensuring that TCN meets the obligations of the Regulation

9.2. Executive Management Committee

- Ensure data protection objectives are established and are aligned with the strategic direction of the Company
- Ensure that the resources needed for the protection of data are available
- Communicate the importance of effective data protection in the Company and of conforming to its requirements
- Support other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility

9.3. Executive Director - General Manager

- Approve any data protection statements attached to communications such as emails and letters
- Approve any data protection queries from journalists or media outlets such as newspaper
- Provide directives that ensure marketing initiatives abide by data protection principles

9.4. Data Protection Officer

- Keep Executive Management updated about data protection responsibilities, risks and issues
- Review all data protection procedures and related policies, in line with an agreed schedule
- Arrange data protection training and advice for the people covered by the Policy
- Handle data protection questions from staff and anyone else covered by the Policy
- Deal with requests from individuals to obtain the data TCN holds about them
- Review and approve any contracts or agreements with third parties that may handle the Company's sensitive data

9.5. Divisional Head, Information Technology

- Ensure all systems, services and equipment used for storing data meet acceptable security standards
- Evaluate any third-party services TCN is considering using to store or process data such as private cloud computing services

9.6. Information Technology Engineers

- Perform regular checks and vulnerability scans to ensure adequate security of hardware and software used in the data processing

9.7. Internal Auditor

- Provide reasonable assurance regarding the achievement of the operational objectives, such as the effectiveness and efficiency of the security controls

9.8. Internal Audit - Central Office Compliance

- Carry out internal audit and report findings to Executive Management Committee
- Recommend preventive and corrective action

10.0 Scope

This Policy applies to all staff, Management and the Board of TCN. As a matter of best practice, other companies (contractors, suppliers etc.), individuals working with TCN and its stakeholders who have access to personal information. It is also applicable to all data that TCN holds relating to identifiable individuals, even if that information technically falls outside of the Regulation. This includes, but is not limited to:

- Names of individuals
- Email addresses
- Contact phone numbers
- ...plus any other information relating to the individuals

11.0 Consequences

The consequence of not adhering to the Policy will be handled in line with the Company's Disciplinary Policy.

12.0 References

Nigeria Data Protection Regulation, 2019.

FIRST APPROVING EXCO MEMBER	SECOND APPROVING EXCO MEMBER
Signature: 	Signature: 
Name: David Kliegl	Name: R Schröder
Designation: General Manager	Designation: Shared Services Manager
Date: 12 April 2022	Date: 12 April 2022