CAPITAL HOTELS PLC

CAPITAL HOTELS PLC

Data Privacy & Protection Policy

Table of Contents

1. INTRODUCTION

As part of our operations, Capital Hotels Plc. ("CHPlc." or "the Company") collects and processes certain types of information (such as name, telephone numbers, address etc.) of individuals that makes them easily identifiable. These individuals include current, past and prospective employees, vendors, guests and other individuals whom CHPlc communicate or deals with, jointly and/or severally ("**Data Subjects**").

Maintaining the Data Subject's trust and confidence requires that Data Subjects do not suffer negative consequences/effects as a result of providing CHPlc. with their Personal Data. To this end, CHPlc. is firmly committed to complying with applicable data protection laws, regulations, rules and principles to ensure security of Personal Data handled by the Company. This Data Privacy & Protection Policy ("**Policy**") describes the minimum standards that must be strictly adhered to regarding the collection, storage, use and disclosure of Personal Data and indicates that CHPlc. is dedicated to processing the Personal Data it receives or processes with absolute confidentiality and security.

This Policy applies to all forms of systems, operations and processes within the CHPlc. environment that involve the collection, storage, use, transmission and disposal of Personal Data.

Failure to comply with the data protection rules and guiding principles set out in the Nigeria Data Protection Regulations 2019 (NDPR) as well as those set out in this Policy is a material violation of CHPlc.'s policies and may result in disciplinary action as required, including suspension or termination of employment or business relationship.

2. SCOPE

This Policy applies to all employees of CHPlc., as well as to any external business partners (such as suppliers, contractors, vendors and other service providers) who receive, send, collect, access, or process Personal Data in any way on behalf of CHPlc., including processing wholly or partly by automated means. This Policy also applies to third-party Data Processors who process Personal Data received from CHPlc.

3. GENERAL PRINCIPLES FOR PROCESSING OF PERSONAL DATA

CHPlc. is committed to maintaining the principles of the NDPR regarding the processing of Personal Data.

To demonstrate this commitment as well as our aim of creating a positive privacy culture within CHPlc, CHPlc adheres to the following basic principles relating to the processing of Personal Data:

3.1 **Lawfulness, Fairness and Transparency**

Personal Data must be processed lawfully, fairly, and transparently always. This implies that Personal Data collected and processed by or on behalf of CHPlc must be in accordance with the specific, legitimate, and lawful purpose consented to by the Data Subject, save where the processing is otherwise allowed by law or within other legal grounds recognized in the NDPR.

3.2 **Data Accuracy**

Personal Data must be accurate and kept up-to-date. In this regard, CHPlc:

a) shall ensure that any data it collects and/or processes is accurate and not misleading in a way that could be harmful to the Data Subject;

b) will make efforts to keep Personal Data updated where reasonable and applicable; and

c) will make timely efforts to correct or erase Personal Data when inaccuracies are discovered.

3.3 **Purpose Limitation**

CHPlc collects Personal Data only for the purposes identified in the appropriate CHPlc Privacy Notice or any other relevant document or based on any other non – written communication (where applicable), provided to the Data Subject and for which Consent has been obtained. Such Personal Data cannot be reused for another purpose that is incompatible with the original purpose, except a new Consent is obtained.

3.4 **Data Minimization**

3.4.1 CHPlc limits Personal Data collection and usage to data that is relevant, adequate, and necessary for carrying out the purpose for which the data is processed.

3.4.2 CHPlc will evaluate whether and to what extent the processing of personal data is necessary, and where the purpose allows, anonymized data must be used.

3.5 **Integrity and Confidentiality**

3.5.1 CHPlc shall establish adequate controls to protect the integrity and confidentiality of Personal Data, both in digital and physical format, and to prevent personal data from being accidentally or deliberately compromised.

3.5.2 Personal data of Data Subjects must be protected from unauthorized viewing or access and from unauthorized changes to ensure that it is reliable and correct.

3.5.3 Any personal data processing undertaken by an employee who has not been authorized to carry such out as part of their legitimate duties is un-authorized.

3.5.4 Employees may have access to Personal Data only as appropriate for the type and scope of the task in question. They are forbidden to use Personal Data for their own private or commercial purposes, disclose it to unauthorized persons, or make it available in any other way.

3.5.5 Human Resources Department must inform employees at the start of the employment relationship about the obligation to maintain personal data privacy. This obligation shall remain in force even after employment has ended.

3.6 Personal Data Retention

3.6.1 All personal information shall be retained, stored and destroyed by CHPlc in line with relevant Legislative and Regulatory Guidelines. CHPlc shall perform periodical reviews of the data retained to confirm the accuracy, purpose, validity, and retention requirements for all Personal Data and records obtained, used and stored within the Company.

3.6.2 To the extent permitted by applicable laws and without prejudice to CHPlc's Retention Policy, the length of storage of Personal Data shall, amongst other things, be determined by:

(a) the contract terms agreed between CHPlc and the Data Subject or as long as it is needed for the purpose for which it was obtained; or

(b) whether the transaction or relationship has statutory implication or a required retention period; or

(c) an express request for deletion by the Data Subject, except where such Data Subject is under an investigation or under a subsisting contract which may require further processing or where the data relates to criminal records; or

(d) whether CHPlc has another lawful basis for retaining that information beyond the period for which it is necessary to serve the original purpose.

Notwithstanding the foregoing and pursuant to the NDPR, CHPlc shall be entitled to retain and process Personal Data for archiving, scientific

research, historical research, or statistical purposes in the public interest.

3.6.3 CHPlc would forthwith delete Personal Data in CHPlc's possession where such Personal Data is no longer required by CHPlc. or in line with CHPlc's Retention Policy, provided no law or regulation being in force requires CHPlc to retain such Personal Data.

3.7 **Accountability**

3.7.1 CHPlc demonstrates accountability in line with the NDPR obligations by monitoring and continuously improving data privacy practices within CHPlc.

3.7.2 Any individual or employee who breaches this Policy may be subject to internal disciplinary action (up to and including termination of employment) and may also face civil or criminal liability if their actions violate the law.

4. DATA PRIVACY NOTICE

4.1 CHPlc considers Personal Data as confidential and, as such, must be adequately protected from unauthorized use and/or disclosure. CHPlc will ensure that the Data Subjects are provided with adequate information regarding the use of their Personal Data as well as acquire their respective Consent, where necessary.

4.2 CHPlc shall display a simple and conspicuous notice (Privacy Notice) on any medium through which Personal Data is being collected or processed. The following information must be considered for inclusion in the Privacy Notice, as appropriate in distinct circumstances in order to ensure fair and transparent processing:

a) Description of collectible Personal Data
b) Purposes for which Personal Data is collected, used and disclosed
c) What constitutes Data Subject's Consent
d) Purpose for the collection of Personal Data
e) The technical methods used to collect and store the information
f) Available remedies in the event of violation of the Policy and the timeframe for remedy.
g) Adequate information in order to initiate the process of exercising their privacy rights, such as access to, rectification and deletion of Personal Data,

5. PURPOSE AND CATEGORY OF DATA COLLECTED AND PROCESSED

5.1. We will only collect and use your Personal data if we have obtained your prior consent or have a lawful and legitimate interest to do so. You are at liberty to withdraw your consent at any time by contacting the Data Protection Officer at notices@abujacontinental.com. The following are data collected and processed by CHPlc:

- Guest data (e.g. name, telephone, e-mail, address, nationality, passport number);
- Key contract data (contractual relationship, product or contractual interest);

- Contract billing and payments data;
- Disclosed information (from third parties);
- Employee and prospective employee data collected for recruitment and onboarding purpose;

5.2. The following are methods adopted by CHPlc in the collection and storage of personal data:

- Registration Form
- Cookies;
- CCTV recordings;

6. LEGAL GROUNDS FOR PROCESSING OF PERSONAL DATA

In line with the provisions of the NDPR, processing of Personal Data by CHPlc shall be lawful if at least one of the following applies:

a) the Data Subject has given Consent to the processing of his/her Personal Data for one or more specific purposes;

b) the processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract;

c) processing is necessary for compliance with a legal obligation to which CHPlc is subject;

d) processing is necessary in order to protect the vital interests of the Data Subject or of another natural person, and

e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official public mandate vested in CHPlc.

7. CONSENT

Where processing of Personal Data is based on consent, CHPlc shall obtain the requisite consent of Data Subjects at the time of collection of Personal Data. In this regard, CHPlc will ensure:

a) that the specific purpose of collection is made known to the Data Subject and that Consent is requested in clear and plain language;
b) that the Consent is freely given by the Data Subject and obtained without fraud, coercion or undue influence;
c) that the Consent is sufficiently distinct from other matters to which the Data Subject has agreed;
d) that the Consent is explicitly provided in an affirmative manner;

e) that Consent is obtained for each purpose of Personal Data collection and processing; and

f) that it is clearly communicated to and understood by Data Subjects that they can update, manage or withdraw their Consent at any time.

7.1 **Valid Consent**

7.1.1 For Consent to be valid, it must be given voluntarily by an appropriately informed Data Subject. In line with regulatory requirements, Consent cannot be implied. Silence, pre-ticked boxes or inactivity does not constitute Consent under the NDPR.

7.1.2 Consent with respect to Sensitive Personal Data must be explicit. A tick of the box would not suffice.

7.2 **Consent of Minors**

The Consent of minors (under 18) will always be protected and obtained from the minor's representatives in accordance with applicable regulatory requirements.

8. DATA SUBJECT RIGHTS

8.1 All individuals who are the subject of Personal Data held by CHPlc are entitled to the following rights:

a) Right to request for and access their Personal Data collected and stored. Where data is held electronically in a structured form, such as in a Database, the Data Subject has a right to receive that data in a common electronic format;

b) Right to information on their personal data collected and stored;

c) Right to objection or request for restriction;

d) Right to object to automated decision making;

e) Right to request rectification and modification of their data which CHPlc keeps;

f) Right to request for deletion of their data, except as restricted by law or CHPlc's statutory obligations;

g) Right to request the movement of data from CHPlc to a Third Party; this is the right to the portability of data; and

h) Right to object to, and to request that CHPlc restricts the processing of their information except as required by law or CHPlc's statutory obligations

8.2 CHPlc's well-defined procedure regarding how to handle and answer Data Subject's requests are contained in CHPlc's Data Subject Access Request Policy.

8.3 Data Subjects can exercise any of their rights by completing the CHPlc's Subject Access Request (SAR) Form and submitting to the Company via notices@abujacontinental.com

9. TRANSFER OF PERSONAL DATA

8.1 Third Party Processor within Nigeria

CHPlc may engage the services of third parties in order to process the Personal Data of Data Subjects collected by the Company. The processing by such third parties shall be governed by a written contract with CHPlc to ensure adequate protection and security measures are put in place by the third party for the protection of Personal Data in accordance with the terms of this Policy and the NDPR.

8.2 Transfer of Personal Data to Foreign Country

8.2.1 Where Personal Data is to be transferred to a country outside Nigeria, CHPlc shall put adequate measures in place to ensure the security of such Personal Data. In particular, CHPlc shall, among other things, conduct a detailed assessment of whether the said country is on the National Information Technology Development Agency (NITDA) Whitelist of Countries with adequate data protection laws.

8.2.2 Transfer of Personal Data out of Nigeria would be in accordance with the provisions of the NDPR. CHPlc will, therefore, only transfer Personal Data out of Nigeria on one of the following conditions:

a. The consent of the Data Subject has been obtained;

b. The transfer is necessary for the performance of a contract between CHPlc and the Data Subject or implementation of pre-contractual measures taken at the Data Subject's request;

c. The transfer is necessary to conclude a contract between CHPlc and a third party in the interest of the Data Subjects;

d. The transfer is necessary for reason of public interest;

e. The transfer is for the establishment, exercise or defence of legal claims;

f. The transfer is necessary to protect the vital interests of the Data Subjects or other persons where the Data Subject is physically or legally incapable of giving consent.

Provided, in all circumstances, that the Data Subject has been manifestly made to understand through clear warnings of the specific principle(s) of data protection that are likely to be violated in the event of transfer to a third country, this proviso shall not apply to any instance where the Data Subject is answerable in duly established legal action for any civil or criminal claim in a third country.

CHPlc will take all necessary steps to ensure that Personal Data is transmitted safely and securely. You will be provided with details of the protection given to your information when it is transferred outside Nigeria upon request.

8.2.3 Where the recipient country is not on the White List, and none of the conditions stipulated in Section 8.2.2 of this Policy is met, CHPlc will engage with NITDA and the Office of the Honourable Attorney General of the Federation (HAGF) for approval with respect to such transfer.

10. DATA BREACH MANAGEMENT PROCEDURE

10.1 A data breach procedure is established and maintained in order to deal with incidents concerning Personal Data or privacy practices leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed.

10.2 All employees must inform their designated line manager or the DPO of CHPlc immediately about cases of violations of this Policy or other regulations on the protection of Personal Data, in accordance with CHPlc's **Personal Data Breach Management Procedure** in respect of any:

a) improper transmission of Personal Data across borders;

b) loss or theft of data or equipment on which data is stored;

c) accidental sharing of data with someone who does not have a right to know this information;

d) inappropriate access controls allowing unauthorized use;

e) equipment failure;

f) human error resulting in data being shared with someone who does not have a right to know; and

g) hacking attack.

10.3 A data protection breach notification must be made immediately after any data breach to ensure that:

a) immediate remedial steps can be taken in respect of the breach;

b) any reporting duties to NITDA or any other regulatory authority can be complied with;

c) any affected Data Subject can be informed; and

d) any stakeholder communication can be managed.

10.4 When a potential breach has occurred, CHPlc will investigate to determine if an actual breach has occurred and the actions required to manage and investigate the breach as follows:

a) Validate the Personal Data breach;

b) Ensure proper and impartial investigation (including digital forensics if necessary) is initiated, conducted, documented, and concluded;

c) Identify remediation requirements and track resolution;

d) Report findings to the top management;

e) Coordinate with appropriate authorities as needed;

f) Coordinate internal and external communications; and

g) Ensure that impacted Data Subjects are properly notified, if necessary.

10.5 You can read more about CHPlc's Personal Data Breach Management Procedure.

11. DATA PROTECTION IMPACT ASSESSMENT

CHPlc shall carry out a Data Protection Impact Assessment (DPIA) in respect of any new project or IT system involving the processing of Personal Data to determine whenever a type of processing is likely to result in any risk to the rights and freedoms of the Data Subject.

CHPlc shall conduct the DPIA according to the procedures laid down in the **CHPlc Data Protection Impact Assessment Policy.**

12. DATA SECURITY

12.1 All Personal Data must be kept securely and should not be stored any longer than necessary. CHPlc will ensure that appropriate measures are employed against unauthorized access, accidental loss, damage and destruction to data. This includes the use of password-encrypted databases for digital storage and locked cabinets for those using paper forms.

12.2 To ensure the security of Personal Data, CHPlc will, among other things, implement the following appropriate technical controls:

a) Industry-accepted hardening standards, for workstations, servers, and databases;

b) Full disk software encryption on all corporate workstation/laptops operating systems drives storing Personal and Personal/Sensitive Data;

c) Encryption at rest including key management of key databases;

d) Enable Security Audit Logging across all systems managing Personal Data;

e) Restrict the use of removable media such as USB flash disk drives;

f) Anonymization techniques on testing environments; and

g) Physical access control where Personal Data are stored in hardcopy.

13. DATA PROTECTION OFFICER

CHPlc has appointed a Data Protection Officer (DPO) responsible for overseeing the Company's data protection strategy and its implementation to ensure compliance with the NDPR requirements. The DPO is knowledgeable in data privacy and protection principles and is familiar with the provisions of the NDPR.

The contact details of the Data Protection officer are as follows –

The Company Secretary
Capital Hotel Plc.
1, Ladi Kwali Way,
Maitama,
Abuja, Nigeria
Samuel.Ozeh@11plc.com

The main tasks of the DPO include:

a) administering data protection policies and practices of CHPlc;

b) monitoring compliance with the NDPR and other data protection laws, data protection policies, awareness-raising, training, and audits;

c) advice the business, management, employees and third parties who carry on processing activities of their obligations under the NDPR;

d) acts as a contact point for CHPlc;

e) monitor and update the implementation of the data protection policies and practices of CHPlc and ensure compliance amongst all employees of CHPlc;

f) ensure that CHPlc undertakes a Data Impact Assessment and curbs potential risk in CHPlc data processing operations; and

g) maintain a Data Base of all CHPlc data collection and processing operations of CHPlc.

14. TRAINING

CHPlc shall ensure that employees who collect, access and process Personal Data receive adequate data privacy and protection training in order to develop the necessary knowledge, skills and competence required to effectively manage the compliance framework under this Policy and the NDPR with regard to the protection of Personal Data. On an annual basis, CHPlc shall develop a capacity-building plan for its employees on data privacy and protection in line with the NDPR.

15. DATA PROTECTION AUDIT

CHPlc shall conduct an annual data protection audit through a licensed Data Protection Compliance Organization (DPCOs) to verify CHPlc's compliance with the provisions of the NDPR and other applicable data protection laws.

The audit report will be certified and filed by the DPCO to NITDA as required under the NDPR.

16. RELATED POLICIES AND PROCEDURES

This Policy shall be read in conjunction with the following policies and procedures of CHPlc:

- Personal Data Breach Management Policy;
- IT Security Policy;
- Document Retention Policy;
- Cookies Policy;
- Privacy Notices; and
- Data Protection Impact Assessment Procedure.

17. CHANGES TO THE POLICY

CHPlc reserves the right to change, amend or alter this Policy at any point in time. If we amend this Policy, we will provide you with the updated version.

18. GLOSSARY

''Consent''	means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, through a statement or a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her.
"Database"	means a collection of data organized in a manner that allows access, retrieval, deletion and processing of that data; it includes but not limited to structured, unstructured, cached and file system type Databases.

"Data Processor	means a person or organization that processes Personal Data on behalf and on instructions of CHPlc.
"DPCO"	means an organization registered by NITDA to provide data protection audit, compliance and training services to public and private organizations that process Personal Data in Nigeria.
"Data Subject"	means any person who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
"NDPR"	means the Nigerian Data Protection Regulation, 2019.
"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 identifier such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM, Personal Identifiable Information (PII) and others.
"**Sensitive Personal Data"**	means data relating to religious or other beliefs, sexual orientation, health, race, ethnicity, political views, trades union membership, criminal records or any other sensitive personal information.

GENERAL INFORMATION

Title	Data Privacy and Protection Policy
Status	Mandatory
Issuing Department	Legal and Compliance
Distribution/Target Audience	All employees, including contracted staff of CHPlc and its subsidiaries, vendors and suppliers of CHPlc.
Approver	Management of CHPlc.
Effective Date	February 2024
Version	1.0

VERSION CONTROL

Version	Last Updated	Reason for Amendment