Privacy and Personal Data Protection Policy

Table of Contents

1. Introduction

In its everyday business operations Check Inn Hotels makes use of a variety of data about identifiable individuals, including data about:

- Current, past and prospective employees
- Customers
- Users of its websites
- Subscribers
- Other stakeholders

In collecting and using this data, the organization is subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it.

The purpose of this policy is to set out the relevant legislation and to describe the steps Check Inn Hotels is taking to ensure that it complies with it.

This control applies to all systems, people and processes that constitute the organization's information systems, including board members, directors, employees, suppliers and other third parties who have access to Check Inn Hotels systems.

2. Privacy and Personal Data Protection Policy

2.1 The Nigerian Data Protection Regulation

The Nigerian Data Protection Regulation 2019 (NDPR) is one of the most significant pieces of legislation affecting the way that Check Inn Hotels carries out its information processing activities. Significant fines are applicable if a breach is deemed to have occurred under the NDPR, which is designed to protect the personal data of citizens of the Federal Republic of Nigeria. It is Check Inn Hotels' policy to ensure that our compliance with the NDPR and other relevant legislation is clear and demonstrable at all times.

2.2 Definitions

There are a total of 24 definitions listed within the NDPR and it is not appropriate to reproduce them all here. However, the most fundamental definitions with respect to this policy are as follows:

"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 and others;*

"Processing" means any operation or set *of operations which is performed on personal data or on 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;*

"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 the manner in which personal data is processed or is to be processed;*

2.3 Principles Relating to Processing of Personal Data

There are a number of fundamental principles upon which the NDPR is based.

These are as follows:

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (Purpose limitation);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (Storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Check Inn Hotels must ensure that it complies with all of these principles both in the processing it currently carries out and as part of the introduction of new methods of processing such as new IT systems. The operation of an information security management system (ISMS) that conforms to the ISO/IEC 27001 international standard is a key part of that commitment.

2.4 Rights of the Individual

The data subject also has rights under the NDPR. These consist of:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Each of these rights must be supported by appropriate procedures within Check Inn Hotels that allow the required action.

2.5. Lawfulness of Processing

There are six alternative ways in which the lawfulness of a specific case of processing of personal data may be established under the NDPR. It is Check Inn Hotels policy to identify the appropriate basis for processing and to document it, in accordance with the regulation. The options are described in brief in the following sections.

2.5. Consent

Unless it is necessary for a reason allowable in the NDPR, explicit consent must be obtained from a data subject to collect and process their data. In case of children below the age of 16 parental consent must be obtained. Transparent information about our usage of their personal data must be provided to data subjects at the time that consent is obtained and their rights with regard to their data explained, such as the right to withdraw consent. This information must be provided in an accessible form, written in clear language and free of charge.

If the personal data are not obtained directly from the data subject then this information must be provided within a reasonable period after the data are obtained and definitely within one month.

2.5.2. Performance of a Contract

Where the personal data collected and processed are required to fulfil a contract with the data subject, explicit consent is not required. This will often be the case where the contract cannot be completed without the personal data in question e.g. a delivery cannot be made without an address to deliver to.

2.5.3. Legal Obligation

If personal data is required to be collected and processed in order to comply with the law, then explicit consent is not required. This may be the case for some data related to employment and taxation for example.

2.5.4. Vital Interests of the Data Subject

In a case where the personal data are required to protect the vital interests of the data subject or of another natural person, then this may be used as the lawful basis of the processing. Check Inn Hotels will retain reasonable, documented evidence that this is the case, whenever this reason is used as the lawful basis of the processing.

2.5.5. Task Carried Out in the Public Interest

Where Check Inn Hotels needs to perform a task that it believes is in the public interest or as part of an official duty then the data subject's consent will not be requested. The assessment of the public interest or official duty will be documented and made available as evidence where required.

2.5.6. Legitimate Interests

If the processing of specific personal data is in the legitimate interests of Check Inn Hotels and is judged not to affect the rights and freedoms of the data subject in a significant way, then this may be defined as the lawful reason for the processing. Again the reasoning behind this view will be documented.

2.6. Privacy by Design

Check Inn Hotels has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect or process personal data will be subject to due consideration of privacy issues, including the completion of one or more privacy impact assessments.

The privacy impact assessment will include:

- Consideration of how personal data will be processed and for what purposes
- Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s)
- Assessment of the risks to individuals in processing the personal data
- What controls are necessary to address the identified risks and demonstrate compliance with legislation

Use of techniques such as data minimization and pseudonymisation will be considered where applicable and appropriate.

2.7. Transfer of Personal Data

Transfers of personal data outside Nigeria must be carefully reviewed prior to the transfer taking place to ensure that they fall within the limits imposed by the NDPR. This depends partly on the Honourable Attorney General of the Federation's (HAGF) judgement as to the adequacy of the safeguards for personal data applicable in the receiving country and this may change over time.

2.8. Data Protection Officer

Check Inn Hotels shall designate a Data Protection Officer (DPO), for the purpose of ensuring adherence to this Regulation, relevant data privacy instruments and data protection directives of the data controller; provided that a data controller may outsource data protection to a verifiably competent firm or person.

2.9. Breach Notification

It is Check Inn Hotels' policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of personal data. In line with the NDPR, where a breach is known to have occurred which is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed within 72 hours. This will be managed in accordance with our I*nformation Security Incident Response Procedure* which sets out the overall process of handling information security incidents.

Under the NDPR the relevant supervisory authority has the ability to impose a range of fines:

a) in the case of a Data Controller dealing with more than 10,000 Data Subjects, payment of the fine of 2% of Annual Gross Revenue of the preceding year or payment of the sum of 10 million naira whichever is greater;

b) in the case of a Data Controller dealing with less than 10,000 Data Subjects, payment of the fine of 1% of the Annual Gross Revenue of the preceding year or payment of the sum of 2 million naira whichever is greater.

3.10. Addressing Compliance to the NDPR

The following actions are undertaken to ensure that Check Inn Hotels complies at all times with the accountability principle of the NDPR:

- The legal basis for processing personal data is clear and unambiguous
- A Data Protection Officer is appointed with specific responsibility for data protection in the organization
- All staff involved in handling personal data understand their responsibilities for following good data protection practice
- Training in data protection has been provided to all staff
- Rules regarding consent are followed

- Routes are available to data subjects wishing to exercise their rights regarding personal data and such enquiries are handled effectively
- Regular reviews of procedures involving personal data are carried out
- Privacy by design is adopted for all new or changed systems and processes
- The following documentation of processing activities is recorded:
  - Organization name and relevant details
  - Purposes of the personal data processing
  - Categories of individuals and personal data processed
  - Categories of personal data recipients
  - Agreements and mechanisms for transfers of personal data to other countries including details of controls in place
  - Personal data retention schedules
  - Relevant technical and organizational controls in place

These actions will be reviewed on a regular basis as part of the management review process of the information security management system.