A subsidiary of Nigerian Breweries Plc.
RC 1189

Progress Trust CPFA Limited

Data Protection Policy

Created: June, 2019

Updated: July, 2021

1. Scope, Applicability and Implementation

1.1 Scope

This Policy addresses the Processing of Personal Data of:

a. Our Employees by Progress Trust CPFA Limited ("the Company") or a Third party on behalf of the Company; and

b. Customers, Suppliers, Business Partners, and other Individuals by the Company or a Third Party on behalf of the Company.

1.2 Electronic and paper-based Processing

This Policy applies to the Processing of Personal Data by written or electronic means and in systematically accessible paper-based filing systems.

1.3 Applicability of local law and Policy

The provisions of the Nigeria Data Protection Regulations (NDPR) 2019 shall govern this Policy as may be applicable from time to time.

1.4 Sub-Policies and Notices

The Company may supplement this Policy through sub-policies or notices that are consistent with the spirit of the Law.

1.5 Accountability

The appropriate Responsible Managers shall be accountable for compliance with this Policy.

1.6 Effective Date

This Policy has been adopted by the Management Team of the Company and shall enter into force as of 3rd June 2019. This Policy shall be published on the Company's website and intranet and shall be made available to Employees and Individuals upon request.

2. Article 2. Purposes for Processing Personal Data

2.1 Legal Basis for Processing Data

Personal Data shall be collected, used or otherwise Processed by the Company for one (or more) of the following the legal basis for Processing data

Employee data

(a) **Human resources and personnel management.** This purpose includes Processing of Personal Data that is necessary for the performance of an employment or other contract with an Employee (or to take necessary steps at the request of an Employee prior to entering into a contract), or for managing the employment-at-will relationship, e.g. management and administration of recruiting and outplacement employability, leave and other absences, compensation and benefits (including pensions), payments, tax issues, career and talent development, performance evaluations, training, travel and expenses, and Employee communications;

(b) **Business process execution and internal management:** This purpose addresses activities such as scheduling work, recording time, managing the Company and Employee assets, provision of central processing facilities for

efficiency purposes, conducting internal audits and implementing business controls, and managing and using Employee directories, archives and insurance proposes, legal or business consulting, and preventing, preparing for or engaging in dispute resolution;

(c) **Organizational analysis and development, management reporting, and acquisitions and divestitures.** This purpose addresses activities such as conducting Employee surveys, managing mergers, acquisitions and divestitures, and Processing Employee Data for management reporting and analysis

2.1.1 Customers, Suppliers and Business Partners Data :

(a) **Assessment and acceptance of Customers, Suppliers and Business Partners:** This purpose includes Processing of Personal Data that are necessary in connection with the assessment and acceptance of Customers, Suppliers and Business Partners including confirming and verifying the identity of relevant Individuals (this may involve the use of a credit reference agency or other Third Parties), conducting due diligence, and screening against publicly available government and/or law enforcement agency sanctions lists;

(b) **Conclusion and execution of agreements with Customers, Suppliers and Business Partners:** This purpose addresses the Processing of Personal Data necessary to conclude and execute agreements with Customers, Suppliers and Business Partners, including required screening activities (e.g. for access to the Company's premises or systems and on compliance with the Heineken Code of Business Conduct), and to record and financially settle delivered services, products and materials to and from the Company. This purpose also includes the Processing of Personal Data in connection with the execution of agreements, including the delivery of Customer Services;

(c) **Development and improvement of products and/or services:** This purpose includes Processing of Personal Data that are necessary for the development and improvement of the Company's products and/or services, research and development;

(d) **Relationship management and marketing:** This purpose includes activities such as maintaining and promoting contact with Customers, Suppliers and Business Partners, account management, customer service, recalls and the development, execution and analysis of market surveys and marketing strategies, including online marketing activities, (e.g. advertising, analysing of online use of the services and the Company website and the purchase of products;

(e) **Business process execution, internal management and management reporting**. This purpose includes the management of company assets, conducting audits and investigations, reviewing and monitoring compliance with Heineken Code of Business Conduct and other terms applicable to the relationship with Customers, Suppliers and Business Partners and other Individuals, finance and accounting, implementing business controls, provision of central processing facilities for efficiency purposes managing mergers, acquisitions and divestitures, and Processing Personal Data for

management reporting and analysis, archive and insurance purposes, legal or business consulting, and preventing, preparing for or engaging in dispute resolution;

2.1.2 Employee data and Customers, Suppliers and Business Partners:

For both Employee and Customers, Suppliers and Business Partners, the legitimate purposes below must be complied with:

(a) **Health, safety, security and integrity**. This purpose includes the protection of the interests of the Company, its Employees, Customers, Suppliers and Business Partners and activities such as those involving health and safety, the protection of the Company and Employee assets, and the authentication of Customer, Supplier or Business Partner status and access rights;

(b) **Compliance with law**. This purpose addresses the Processing of Personal Data necessary for the performance of a task carried out to comply with a legal obligation or sectorial recommendation to which the Company is subject, including the disclosure of Personal Data to government institutions or supervisory authorities, including tax authorities, in relation thereto; or

(c) **Protection of the vital interests of Employees and Individuals.** This is where Processing is necessary to protect the vital interests of an Employee or Individual.

Where there is a question whether a Processing of Personal Data can be based on a Business Purpose listed above, the Data Protection Officer will be consulted before the Processing takes place.

2.2 Consent

The Company shall (also) seek consent from the Employee or Individual for the Processing. Where consent is not obtained but the Processing is reasonably necessary to address a request of the individual (e.g. he subscribes to a service or seeks a benefit), the lawful basis for processing would be the performance of a contract or processing based on the request of the Employee or Individual

When seeking consent, the Company must inform the Employee or Individual:
(a) of the purposes of the Processing for which consent is required;
(b) of the possible consequences of the Processing;
(c) who is responsible for the Processing; and
(d) that he or she is free to refuse or withdraw consent at any time during the term of the employment or contract; and
(e) that withdrawal of consent does not affect the lawfulness of the relevant Processing before such withdrawal.

2.3 Denial or withdrawal of consent

The Employee or Individual may either deny consent and/or withdraw consent at any time. The withdrawal of consent shall not affect the lawfulness of the Processing based on such consent before its withdrawal.

3. Article 3. Use for Other Purposes

3.1 Use of Data for Secondary Purposes

Personal Data may be processed for further use of the Company different from the Original Purpose (Secondary Purpose) only if the Original Purpose and Secondary Purpose are closely related, provided that the data subject consents to such further processing or the processing is required in compliance with a legal obligation. Depending on the sensitivity of the relevant Personal Data, and whether use of the Data for the Secondary Purpose has potential negative consequences for the Employee or Individual, the use of Secondary Purpose may require additional measures such as:

(a) limiting access to the Data;
(b) imposing additional confidentiality requirements;
(c) taking additional security measures;
(d) obtaining specific consent from the Individual about the Secondary Purpose;
(e) providing an opt-out opportunity; or
(f) obtaining an Employee or Individual's consent in accordance with Article 2.2 or Article 4.3, where applicable.

4. Article 4. Purposes for Processing Sensitive Data

4.1 Specific purposes for Processing Sensitive Data

The Company shall Process Sensitive Data only to the extent necessary to serve the applicable Business Purpose. The following categories of Sensitive Data may be collected, used or otherwise Processed only for one (or more) of the purposes specified below:

(a) ***Racial or ethnic data:*** *This will include:*

(i) photos and video images of the Employee or Individual, for the protection of the Company and Employee assets, including screening and monitoring of Employees before and during employment, to verify and confirm advice or recorded decisions made in the course of business for future reference, for site access and security reasons and employee directories;
(ii) providing preferential status to persons from particular ethnic or cultural minorities to remove or reduce inequality or to ensure diversity in staffing, provided that the use of the relevant Sensitive Data allows for an objective determination that an Employee belongs to a minority group and the Employee has not filed a written objection against the relevant Processing.
(iii) administering Employee affinity groups.
(iv) for assessment and acceptance of Customers including the identification and authentication of Customers (including confirming and verifying the identity of relevant Individuals);
(v) for assessment and verification of Supplier or Business Partner status and access rights; and
(vi) for verifying and confirming advice provided by the Company to Individuals (e.g. when Individuals participate in video conferencing which is recorded);

(b) ***Physical or mental health data*** *(including any opinion of physical or mental health and data relating to disabilities and absence due to illness or pregnancy*):

(i) providing health services to an Employee provided that the relevant health data are processed by or under the supervision of a health professional who is subject to professional confidentiality requirements;

(ii) administering pensions, health and welfare benefit plans, maternity, paternity or family leave programs, or collective agreements (or similar arrangements) that create rights depending on the state of health of the Employee;

(iii) providing preferential status to persons with a particular disability to remove or reduce inequality or to ensure diversity in staffing, provided that use of the relevant Sensitive Data allows for an objective determination that an Employee belongs to the relevant category and the Employee has not filed a written objection against the relevant Processing;

(iv) reintegrating or providing support for Employees entitled to benefits in connection with illness or work incapacity;

(v) for screening and monitoring of Employees before and during employment and for assessing and making decisions on (continued) eligibility for positions, projects or scope of responsibilities; or

(vi) providing facilities in the workplace to accommodate health problems or disabilities.

(c) ***Criminal data (including data relating to criminal behaviour, criminal records or proceedings regarding criminal or unlawful behaviour):***

(i) assessing an application by an Employee to make a decision about the Employee or provide a service to the Employee; or

(ii) protecting the interests of the Company or its Employees with respect to criminal offences that have been or, given the relevant circumstances are suspected to be or have been, committed against the Company or its Employees, and for screening and monitoring of Employees before and during employment.

(iii) for assessment and acceptance of Customers, Suppliers and Business Partners, including the identification and authentication of Customers (including confirming and verifying the identity of relevant Individuals);

(iv) for the execution of an agreement with Customers; and further

(v) for protecting the interests of the Company, its Employees, Customers, Suppliers and Business Partners;

(d) ***Sexual preference*** (including data relating to partners of Employees):

(i) administering Employee pensions and benefits programs; or (ii) administering Employee memberships.

(e) ***Religion or philosophical beliefs:***

(i) accommodating Employees' religious or philosophical practices, dietary requirements or religious holidays.
(ii) accommodating specific products or services for a Customer and to accommodate dietary requirements or religious holidays e.g. for Customer, Supplier or Business Partner events.

4.2 General purposes for Processing Sensitive Data

In addition to the specific purposes listed in Article 4.1 above, all categories of Sensitive Data may be Processed under one (or more) of the following circumstances:

(a) as required or allowed for the performance of a task carried out to comply with a legal obligation or sectorial recommendation to which the Company is subject;
(b) by or allowed under applicable law;
(c) for the establishment, exercise or defence of a legal claim;
(d) to protect a vital interest of an Employee or Individual, but only where it is impossible to obtain the Employee or Individual's consent first;
(e) to the extent necessary to comply with an obligation of international public law (e.g. treaties);
(f) where Sensitive Data have manifestly been made public by the Employee or Individual; or
(g) to the extent necessary for reasons of substantial public interest.

4.3 Consent, and the denial or withdrawal thereof

(a) Employee consent generally cannot be used as a legitimate basis for Processing Sensitive Data. One of the grounds listed in Article 4.1 or 4.2 must exist for any Processing of Sensitive Data. The Company shall also seek the Employee or Individual's consent for the Processing. If none of the grounds listed in Article 4.1 or 4.2 applies, the Company may request Employee consent for Processing Sensitive Data, but only if the Employee or Individual has given explicit consent to the Processing thereof, and in the case of an Employee, Processing has no foreseeable adverse consequences for the Employee (e.g. Employee diversity programs or networks, research, product development, selection of candidates in hiring or management development processes). Article 2.3 applies to the granting, denial or withdrawal of Employee consent

4.4 Prior Authorization of Data Protection Officer

Where Sensitive Data are Processed based on a requirement of a law other than the Nigerian Data Protection Regulations, or based on the consent of the Employee applicable to the Processing, the Processing requires prior authorization Data Protection Officer.

4.5 Use of Sensitive Data for Secondary Purposes

Sensitive Data of Employees (or their dependants) and Individuals may be Processed for Secondary Purposes in accordance with Article 3.

5. Article 5. Quantity and Quality of Data

5.1 No Excessive Data

The Company shall restrict the Processing of Employee and Individual Personal Data to those Data that are reasonably adequate for and relevant to the applicable Business Purpose. The Company shall take reasonable steps to delete Personal Data that are not required for the applicable Business Purpose.

5.2 Storage and data retention period

The Company shall generally retain Personal Data only for the period required to serve the applicable Business Purpose, to the extent reasonably necessary to comply with an applicable legal requirement, or as advisable in light of an applicable statute of limitations. The Company may specify (e.g., in a sub-policy, notice or records retention schedule) a time period for which certain categories of Personal Data may be kept.

Promptly, after the applicable retention period has ended, the Data Protection Officer shall direct that the Data be:

(a) securely deleted or destroyed;
(b) de-identified; or
(c) transferred to an Archive as agreed from time to time.

5.3 Quality of Data

Personal Data should be accurate, complete and kept up-to-date to the extent reasonably necessary for the applicable Business Purpose.

5.4 Privacy by Design

The Company shall take commercially reasonable technical and organizational steps to ensure that the requirements of this Article 5 are implemented into the design of new systems and processes that Process Personal Data.

5.6 Accurate, complete and up-to-date Data

It is the responsibility of Employees and Individuals to ensure that their Personal Data, as held by the Company, are accurate, complete and up-to-date. Employees and Individuals shall inform the Company regarding any changes in accordance with Article 7.

6. Article 6. Employee and Individual Information Requirements

Information requirements

The Company shall inform Employees and Individuals through a notice of the following information, unless the person already has the information:

(a) the Business Purposes (including Secondary Purposes) for which their Data are Processed;
(b) the categories of Third Parties to which the Data are disclosed (if any) and whether any Third Party is located in a country outside Nigeria which Third Party or country is not covered by an Adequacy Decision; and
(c) other information where relevant, which include:

(i) the nature and categories of the Processed Data;
(ii) the period for which the Data will be stored or (if not possible) the criteria used to determine this period;
(iii) an overview of the rights of Employees and Individuals under this Policy and how these can be exercised;
(iv) the existence of automated decision making referred to in Article 10.1 as well as meaningful information about the logic involved and potential negative consequences thereof for the Employee or Individual;
(v) the source of the Data (where the Personal Data have not been obtained from the Employee or Individual), including whether the Personal Data came from a public source.

7. Article 7. Individual Rights of Access and Rectification and Erasure

7.1 Rights of Employees and Individuals

Every Employee and Individual has the right to request a copy of his Personal Data Processed by or on behalf of the Company and further, where reasonably possible as contained in Article 6(d) above.

If the Personal Data are incorrect, incomplete or not Processed in compliance with the NDPR or this Policy, the Person has the right to have his Data rectified, deleted or the Processing thereof restricted (as appropriate).

In addition, the Person has the right to object to:

(a) the Processing of his/her Data on the basis of grounds related to his particular situation, unless the Company can demonstrate a prevailing legal basis for the Processing; and
(b) the Processing of his/her Data for direct marketing communications, including profiling to the extent that it is related to such direct marketing.

The Person has the right (at his option) to receive a copy of the Data that he has provided in a common machine readable format or in writing. It shall be in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means.

7.2 Procedure

The Employee or Individual shall send his request to the contact person or contact point indicated in the relevant Privacy Policy or notice.

Prior to fulfilling the request of the Person, the Company may require the Person to:
(a) specify the categories of Personal Data to which he is seeking access;
(b) specify to the extent reasonably possible the data system in which the Data are likely to be stored;
(c) specify the circumstances in which the Company obtained the Personal Data;
(d) provide proof of his identity when the Company has reasonable doubts concerning such identity, or to provide additional information enabling his identification;

(e) pay a fee to compensate the Company for the reasonable costs relating to fulfilling the request, provided the Company can reasonably demonstrate that the request is manifestly unfounded or excessive, e.g. because of its repetitive character; and
(f) in case of a request for rectification, deletion, or blockage, specify the reasons why the Personal Data are incorrect, incomplete or not Processed in accordance with the NDPR or this Policy.

7.3 Response period

Within one month of the Company receiving the request, the contact person, contact point, or Data Protection Officer shall inform the Individual in writing or electronically either:

(i) of the Company's position with regard to the request and any action the Company has taken or will take in response; or
(ii) the ultimate date on which he will be informed of the Company's position and the reason for the delay, which date will be no later than eight (8) weeks after the communication was sent to the Individual.

7.4 Complaint

An Employee or Individual may file a complaint in accordance with Article 16.3 if:

(a) the response to the request is unsatisfactory to the Person (e.g. the request is denied);
(b) the Person has not received a response as required by Article 7.3; or
(c) the time period provided to the Person in accordance with Article 7.3 is, in light of the relevant circumstances, unreasonably long and the Person has objected but has not been provided with a shorter, more reasonable time period in which he will receive a response.

7.5 Denial of requests

The Company may deny an Employee or Individual's request if:

- the request does not meet the requirements of Articles 7.1 and 7.2;
- the request is not sufficiently specific;
- the identity of the relevant Person cannot be established by reasonable means, including the additional information provided by the Employee or Individual;
- The Company can reasonably demonstrate that the request is manifestly unfounded or excessive, e.g. because of its repetitive character. A time interval between requests of six months or less shall generally be deemed to be an unreasonable time interval; or
- the request violates the rights of other Employees or individuals.

7.6 No requirement to Process identifying information

The Company is not obliged to Process additional information in order to be able to identify the Employee or Individual for the sole purpose of facilitating the rights of the Individual under this Article 7.

8. Article 8. Security and Confidentiality Requirements

8.1 Data security

The Company shall take appropriate commercially reasonable technical, physical and organizational measures to protect Personal Data from misuse or accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure, acquisition or access. To achieve this, the Company has developed and implemented an Information Technology Security Policy and other policies relating to the protection of Personal Data.

8.2 Staff access

Staff members shall be authorized to access Employee and Individual Personal Data only to the extent necessary to serve the applicable Business Purpose and to perform their job.

8.3 Confidentiality obligations

Staff members who access Personal Data must meet their confidentiality obligations.

8.4 Data Security Breach notification requirement

The Company shall notify the Employee or Individual of a Data Security Breach within a reasonable period of time following discovery of such breach, unless a law enforcement official or supervisory authority determines that notification would impede a (criminal) investigation or cause damage to national security. In this case, notification shall be delayed as instructed by such authority. The Company shall respond promptly to inquiries of Employees and Individuals relating to such Data Security Breach.

8.5 Available remedies in the event of violation of Privacy Policy

All suspected Data Breach incidents must be reported immediately it is identified to the designated line manager or Data Protection Officer (“DPO”) to ensure that:

a. any reporting duties under the Nigeria Data Protection Regulation, 2019 (NDPR) and other applicable laws can be complied with;
b. any affected Data Subject can be informed; and
c any stakeholder communication can be managed.

Time frame for remedy

In the event of any data breach incident, PTL shall notify NITDA within **72 hours** of the knowledge of the breach, in line with the provisions of the NDPR. The report would detail the number of data likely to be affected, cause of the breach and remedial actions being taken by PTL to remedy the breach.

In particular, the notification to NITDA will include the following:

a. A description of the circumstances of the loss or unauthorized access or disclosure;
b. The date or time period during which the loss or unauthorized access or disclosure occurred or continued;
c. A description of the personal information involved in the loss or unauthorized access or disclosure;
d. An assessment of the risk of harm to individuals as a result of the loss or unauthorized access or disclosure;
e. 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;
f. A description of any steps PTL has taken to reduce the risk of harm to individuals;
g. A description of any steps PTL has taken to notify individuals of the loss or unauthorized access or disclosure, and
h. The name and contact information for a person who can answer (such as the DPO), on behalf of PTL's NITDA's questions about the loss of unauthorized access or disclosure.

In addition to any notification to NITDA and based on the evaluation of risks and consequences, the DPO shall determine whether it is necessary to notify the Data Subject(s) about the Data Breach incident. The report to the affected Data Subject shall be in the prescribed Data Breach Notification Form.

Before any external report is made (whether to NITDA or Data Subject), relevant stakeholders and in particular the PTL's Data Breach Management Team need to be engaged in the drafting of the relevant notification and to also ensure that PTL can adequately deal with any external inquiries that may be directed at the Company as a result of the breach.

9. Article 9. Direct Marketing

9.1 Direct marketing

This Article sets forth requirements concerning the Processing of Personal Data for direct marketing purposes (e.g. contacting the Individual by email, fax, phone, SMS or otherwise, with a view of solicitation for commercial or charitable purposes).

9.2 Consent for direct marketing (opt-in)

(a) If applicable law so requires, the Company shall only send to Persons unsolicited commercial electronic communication with the prior consent of the Individual ("opt-in"). If applicable law does not require prior consent of the Person, the

Company shall in any event offer the Person the opportunity to opt-out of such unsolicited commercial communication.

(b) Exception (opt-out)
Prior consent of the Person for sending unsolicited commercial electronic communication is not required if a Person clearly and distinctly has been given the opportunity to object free of charge, and in an easy manner, to such use of his electronic contact details when they are collected by the Group Company.
(c) Information to be provided in each communication
In every direct marketing communication that is made to the Person, the Individual shall be offered the opportunity to opt-out of further direct marketing communications.

(d) Objection to direct marketing
If an Individual objects to receiving marketing communications from the Company, or withdraws his consent to receive such communications, the Company will take steps to refrain from sending further marketing materials as specifically requested by the Individual. The Company will do so within a reasonable time frame.

(e) Third Parties and Direct marketing
No Data shall be provided to, or used on behalf of, Third Parties for purposes of direct marketing of such Third Party without the prior consent of the Person.

(f) Personal Data of Children
The Company shall not use any Personal Data of Children for direct marketing, without the prior consent of their parent or custodian.

(g) Direct marketing records
The Company shall keep a record of Persons that used their "opt-in" or "opt-out" right and will regularly check the public opt-out registers.

10. Article 10. Automated Decision Making (including profiling)

10.1 Automated decisions

Automated tools may be used to make decisions about Employees and Individuals but decisions with a negative outcome for the Employee and Individual may not be based solely on the results provided by the automated tool. This restriction does not apply if:

(a) the use of automated tools is necessary for the performance of a task carried out to comply with a legal obligation or sectorial recommendation to which the Company is subject;
(b) the decision is made by the Company for purposes of:
  (i) entering into or performing a contract; or
  (ii) managing the contract, provided the underlying request leading to a decision by the Company was made by the Employee or Individual (e.g. where automated tools are used to filter promotional game submissions); or
(c) the Employee or Individual has given his explicit consent

In case Article 10 (b) or (c) is applicable, the Company shall take suitable measures to safeguard the legitimate interests of the Employee or Individual, e.g. by providing the Employee or Individual with an opportunity to express his/her point of view.

11. Article 11. Transfer of Personal Data to Third Parties

11.1 Transfer to Third Parties

This Article sets forth requirements concerning the transfer of Personal Data from the Company to a Third Party. Note that a transfer of Personal Data includes situations in which the Company discloses Personal Data to Third Parties (e.g., in the context of corporate due diligence) or where the Company provides remote access to Personal Data to a Third Party.

11.2 Third Party Processors and Third Party Controllers

(a) **Third Party Processors:** these are Third Parties that Process Personal Data solely on behalf of the Company and at its direction (e.g., Third Parties that Process online registrations made by Customers or process Employee salaries on behalf of the Company);

(b) **Third Party Controllers:** these are Third Parties that Process Personal Data and determine the purposes and means of the Processing (e.g. Business Partners that provide their own goods or services directly to Customers, government authorities or service providers that provide services directly to Employees).

11.3 Transfer for applicable Business Purpose only

The Company shall transfer Personal Data to a Third Party to the extent necessary to serve the applicable Business Purpose (including Secondary Purposes as per Article 3 or purposes for which the Employee or Individual has provided consent in accordance with Article 2).

11.4 Third Party Controller safeguards

Third Party Controllers (other than government agencies) may Process Personal Data only if they have a written contract with the Company. In the contract, the Company shall seek to contractually protect the data and privacy interests of its Employees or Individuals when Personal Data are transferred to Third Party Controllers. All such contracts shall be drafted in consultation with the Data Protection Officer.

11.5 Third Party Processor contracts

Third Party Processors may Process Personal Data only if they have validly entered into written or electronic contract with the Company (Processor Contract). The contract with a Third Party Processor must include the following provisions:

(a) the Third Party Processor shall Process Personal Data only in accordance with the Company's instructions including on transfers of Personal Data to

any Third Party Processor located in a country outside Nigeria and which Third Party Processor or country are not covered by an Adequacy Decision, unless the Third Party Processor is required to do so under mandatory requirements applicable to the Third Party Processor and for the purposes authorised by the Company;

(b) the Third Party Processor shall keep the Personal Data confidential;

(c) the Third Party Processor shall take appropriate technical, physical and organizational security measures to protect the Personal Data;

(d) the Third Party Processor shall only permit subcontractors to Process Personal Data in connection with its obligations to the Company:
   (i) with the prior specific or generic consent of the Company, and
   (ii) based on a validly entered into written or electronic contract with the subcontractor, which imposes similar privacy protection-related Processing terms as those imposed on the Third Party Processor under the Processor Contract, and provided that the Third Party Processor remains liable to the Company for the performance of the subcontractor in accordance with the terms of the Processor Contract;

(e) The Company has the right to review the security measures taken by the Third Party Processor and the Third Party Processor shall subject its relevant data processing facilities to audits and inspections by the Company, a Third Party on behalf of the Company or any relevant government authority;

(f) the Third Party Processor shall promptly inform the Company of any actual or suspected Data Security Breach involving Personal Data; and

(g) the Third Party Processor shall deal promptly and appropriately with
   (a) inquiries of the Company related to the Processing of Personal Data; and
   (b) requests for assistance of the Company, as reasonably required to ensure compliance of the Processing of Personal Data with applicable law;

(h) upon termination of the Processor Contract, the Third Party Processor shall, at the option of the Company, return the Personal Data and copies thereof to the Company or shall securely delete such Personal Data, except to the extent the Processor Contract or applicable law provides otherwise.

11.6 Transfer of Data to Third Parties outside Nigeria

This Article sets forth additional rules for Personal Data that are:

- collected originally in connection with activities of the Company that is located outside Nigeria; and
- transferred to a Third Party that is located in a country outside Nigeria

Any transfer of personal data which are undergoing processing or are intended for processing after the transfer to a foreign country or to an International Organization shall take place subject to the supervision of the Honourable Attorney General of the Federation of Nigeria.

Personal Data may be transferred to such a Third Party only if:

a) that the Data Subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers;

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

c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Controller and another natural or legal person;

d) the transfer is necessary for important reasons of public interest;

e) the transfer is necessary for the establishment, exercise or defence of legal claims; and

f) the transfer is necessary in order 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;

g) the transfer is necessary to satisfy a Business Purpose of the Company, provided the transfer is not repetitive, concerns only a limited number of Employees or Individuals, and the interests of the affected Individuals do not outweigh the Business Purpose for which the transfer is made.

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."

Items 11.6 (d), (e) and (g) above require the prior approval of the Global Privacy Officer.

11.7 Consent to transfer

a. Employee

The Company generally shall not seek Employee consent for a transfer of Employee Data to a Third Party located outside Nigeria and the Third Party or country are not covered by an Adequacy Decision. One of the grounds for transfer listed in Article 11.6 must exist. If none of the grounds listed in Article 11.6 exists, the Company may request Employee consent for a transfer to a Third Party located in a country outside Nigeria and the Third Party or country are not covered by an Adequacy Decision, but only if:

(i) the transfer has no foreseeable adverse consequences for the Employee; or

(ii) the consent is requested prior to the participation of the Employee in specific projects, assignments or tasks that require the transfer of the Data.

Requesting Employee consent for a transfer requires the prior approval of the Data Protection Officer. Prior to requesting Employee consent, the Employee shall be provided with the following information:

(i) the purpose of the transfer;
(ii) the identity or categories of Third Parties to which the Data will be transferred;
(iii) the categories of Data that will be transferred;
(iv) the country to which the Data will be transferred; and
(v) the fact that the Data will be transferred to a Third Party located in a country outside Nigeria which Third Party or country is not covered by an Adequacy Decision.

The requirements set out in Articles 2.2 and 2.3 apply to the requesting, denial or withdrawal of Employee consent.

b. Other individuals

If none of the grounds listed in Article 11.6, prior to requesting consent, the Individual shall be provided with the following information:

(i) the purpose of the transfer;
(ii) the identity or categories of Third Parties to which the Data will be transferred;
(iii) the categories of Data that will be transferred;
(iv) the country to which the Data will be transferred; and
(v) the fact that the Data will be transferred to a Third Party located in a country outside Nigeria which Third Party or country is not covered by an Adequacy Decision.

The requirements set out in Articles 2.2 and 2.3 apply to the requesting, denial or withdrawal of consent.

12. Article 12. Overriding Interests

12.1 Overriding interests

The obligations of the Company and rights of Individuals as specified in Articles 12.2 and 12.3 may be overridden if, under the specific circumstances at issue, a pressing need exists that outweighs the interest of the Individual (Overriding Interest). An Overriding Interest exists if there is a need to:

(a) Take any of the following steps:
  (i) the health, security or safety of Employees or Individuals;
  (ii) the Company's intellectual property rights, trade secrets or reputation;
  (iii) The Company's business operations;
  (iv) the preservation of confidentiality in a proposed sale, merger or acquisition of a business; or
  (v) the involvement of trusted advisors or consultants for business, legal, tax, or insurance purposes.
(b) prevent or investigate (including cooperating with law enforcement) suspected or actual violations of law, breaches of the terms of contract, or

non-compliance with the Heineken's Code of Business Conduct or other Company policies and procedures; or

(c) otherwise protect or defend the rights or freedoms of the Company, its Employees or other persons.

12.2 Exceptions in the event of Overriding Interests

If an Overriding Interest exists, one or more of the following obligations of the Company or rights of the Individual may be set aside:

(a) Article 3.1 (the requirement to Process Personal Data for closely related purposes);

(b) Article 6 (information provided to Employees and Individuals, Personal Data not obtained from the Employees or Individuals);

(c) Article 7 (rights of Employees and Individuals);

(d) Articles 8.2 and 8.3 (Staff access limitations and confidentiality requirements); and

(e) Articles 11.4, 11.5 and 11.6(b) (contracts with Third Parties).

12.3 Sensitive Data

The requirements of Articles 4.1 and 4.2 (Sensitive Data) may be set aside only for the Overriding Interests listed in Article 12.1(a)(i), 12.1(a)(ii), 12.1(a)(iii), 12.1(a)(v), 12.1(b) and 12.1(c).

12.4 Consultation with the Data Protection Officer

Setting aside obligations of the Company or rights of Individuals based on an Overriding Interest requires prior consultation with the Data Protection Officer. The Data Protection Officer shall document his advice.

12.5 Information to Employee or Individual

Upon request of the Employee or Individual, the Company shall inform the Person of the Overriding Interest for which obligations of the Company or rights of the Employee or Individual have been set aside, unless the particular Overriding Interest sets aside the requirements of Articles 6.1 or 7.1, in which case the request shall be denied.

13. Article 13. Supervision and Compliance

13.1 Data Protection Officer

The Company shall appoint a Data Protection Officer who is responsible for:

(a) Supervising compliance with this Policy;

(b) Coordinating, communicating and consulting with the Global Privacy Office on central data protection issues;

(c) Providing annual privacy / data protection reports, as appropriate, to the regulators in line with the Data Protection Regulation and to the

Management team on data protection risks and compliance issues, and as described in article 16.2;

(d) Coordinating, in conjunction with the relevant persons in the Company, official investigations or inquiries into the Processing of Personal Data by a government authority;

(e) Monitoring the documentation, notification and communication of Data Security Breaches;

(f) Deciding on complaints as described in Article 17; and creating and maintaining a framework for:

(i) updating of local data protection policies and procedures;
(ii) the maintaining, updating and publishing of this Policy and related subpolicies;
(iii) the monitoring, auditing and reporting on compliance with this Policy to the management team;
(iv) the collecting, investigating and resolving privacy inquiries, concerns and complaints; and
(v) determining and updating appropriate measures/sanctions for violations of this Policy (e.g. disciplinary standards);

(a) Support and assess overall data protection management compliance within the Company;

(b) Regularly advise their respective management teams, Responsible Managers and the Global Privacy Officer on data protection & privacy risks and compliance issues;

(c) Be available for requests for privacy and data protection approvals or advice as described in Articles 2.1, 2.2, 4.4, Article 7 and 11.7;

(d) Provide information relevant to the annual privacy report of the Global Privacy Officer (as required in Article 16;

(e) Direct that stored Personal Data be deleted or destroyed, de-identified or transferred as required by Article 5.2;

(f) Decide on and notify the Global Privacy Officer of complaints as described in Article 17; and

13.2 Responsible Managers

The Responsible Managers are accountable that effective data protection management is implemented in the Company (including but not limited to the obligation to appoint a Data Protection & Privacy Officer and the responsibility for executing Privacy Impact Assessments, where necessary), is integrated into business practices, and that adequate resources and budget are available.

The Responsible Managers shall be accountable for:

(a) Ensuring overall data protection management compliance within the Company, also during and following organisational restructuring, outsourcing, mergers and acquisitions and divestures;

(b) Implementing the data management processes, systems and tools, devised by the Global Privacy Office to implement the framework for data protection management in the Company;

(c) Ensuring that the data protection management processes and systems are maintained up to date against changing circumstances and legal and regulatory requirements;

(d) Ensuring and monitoring ongoing compliance of third parties with the requirements of this Policy in case Personal Data are disclosed by the Company to a Third Party (including entering into a written or electronic contract with such Third Party and obtaining a sign off of such contract from the legal department);
(e) Ensuring that relevant persons in the Company follow the prescribed data protection training courses; and
(f) Directing that stored Personal Data be deleted or destroyed, de-identified or transferred as required by Article 5.2.
(g) Appointing a Data Protection Officer for the Company;
(h) Informing the Global Privacy Office of any new legal requirement that may interfere with the Company's ability to align with the Global Privacy requirements.

14. Article 14. Policies and Procedures

14.1 Policies and procedures

The Company shall review and update this Policy, as may be required at least once every two years or as often as may be necessary to align with the Nigerian legislation and changes to the law from time to time.

14.2 System information

The Company shall maintain readily available information regarding the structure and functioning of all systems and processes that Process Personal Data (e.g. inventory of systems and processes).

15. Article 15. Training

Staff training

The Company shall provide training on this Policy and related confidentiality obligations to Staff members who have access to Personal Data.

16. Article 16. Monitoring and Auditing Compliance

16.1 Audits

The Company's Internal Audit team shall assess business processes and procedures that involve the Processing of Personal Data for compliance with this Policy. The audits shall be carried out in the course of the regular activities of the Audit Team or at the request of the Data Protection Officer. The Management team of the Company and the Global Privacy Office shall be informed of the results of the audits. A copy of the audit results will be provided to the National Information Technology Development Agency (NITDA) as required by law.

16.2 Annual Data Protection / Privacy Report

The Data Protection Officer shall implement appropriate processes to monitor compliance with this Policy and produce an annual Data Protection / privacy report on compliance with the Policy, data protection risks and other relevant issues. Copies of the Report shall be made available to the Global Privacy Office.

16.3 Mitigation

The Company shall, if so indicated, ensure that adequate steps are taken to address breaches of this Policy identified during the monitoring or auditing of compliance pursuant to this Article 16.

17. Article 17. Complaints Procedure

17.1 Complaint

Employees and Individuals may file a complaint regarding compliance with this Policy or violations of their rights under Data Protection laws:
(a) in accordance with the applicable complaints procedure set forth in the Heineken's Code of Business Conduct (Speak-Up) or contract; or (b) with the Data Protection Officer.

The Data Protection Officer shall, with the approval of the Responsible Managers:
(c) notify the Global Privacy Office;
(d) initiate an investigation; and
(e) when necessary, advise the business on the appropriate measures for compliance and monitor, through to completion, the steps designed to achieve compliance.

The Data Protection Officer may consult with any government authority having jurisdiction over a particular matter about the measures to be taken.

17.2 Reply to Employee or Individual

Within four weeks of the Company receiving a complaint, the Data Protection Officer shall inform the Employee or Individual in writing, or electronically either:

(i) of the Company's position with regard to the complaint and any action the Company has taken or will take in response, or

(ii) when he will be informed of the Company's position, which date shall be no later than twelve weeks thereafter. The Data Protection Officer shall send a copy of the complaint and his written reply to the Global Privacy Office.

17.3 Complaint to Global Privacy Officer

An Employee or Individual may file a complaint with the Global Privacy Officer if:
(a) the resolution of the complaint by the Data Protection Officer is unsatisfactory to the Employee or Individual (e.g. the complaint is rejected)
(b) the Individual has not received a response as required by Article 17.2;
(c) the time period provided to the Individual pursuant to Article 17.2 is, in light of the relevant circumstances, unreasonably long and the Individual has objected, but has not been provided with a shorter, more reasonable time period in which he will receive a response; or (d) in the events listed in Article 7.4.

The Policy described in Articles 17.1 and 17.2 shall apply to complaints filed with the Global Privacy Office.

18. Article 18. Legal Issues

18.1 Complaints procedure

Employees and Individuals are encouraged to first follow the complaints procedure set forth in Article 17 of this Procedure before filing any complaint or claim with the NITDA or the Courts.

18.2 Local law and jurisdiction

The rights contained in this Article are in addition to and shall not prejudice any other rights or remedies that either party may otherwise have by law.

In case of a violation of this Policy, the Employee or Individual may only, at his choice, submit a complaint or a claim, as applicable, to:

(a) NITDA
(b) High Court of competent jurisdiction

The NITDA and High Courts shall apply their own substantive and procedural laws to the dispute. Any choice made by the Employee or Individual will not prejudice the substantive or procedural rights he or she may have under applicable law.

18.3 Right to claim direct damages

In case an Employee or Individual brings a claim under Article 18.2, such Individual shall be entitled to compensation of damages, to the extent provided by the applicable law, suffered by an Individual resulting from a violation of this Policy.

18.4 Burden of proof in respect of claim for damages

In case an Employee or Individual brings a claim for damages under Article 18.2, it will be for the Employee or Individual to demonstrate that he has suffered actual damages and to establish facts which show it is plausible that the damage has occurred because of a violation of this Policy. It will subsequently be for the Company to prove that the damages suffered by the Employee or Individual due to a violation of this Policy are not attributable to the Company.

19. Article 19. Sanctions for Non-compliance

Non-compliance of Employees or Individuals with this Policy may result in appropriate measures in accordance with applicable law up to and including termination of employment and contract.

20. Article 20. Changes to the Policy

20.1 Any changes to this Policy require the prior approval of the Management Team of the Company. The Company shall notify the NITDA as appropriate where there are any material changes to this Policy.

20.2 This Policy may be changed by the Company without the Employee or Individual's consent even though an amendment may relate to a benefit conferred on the Employees or Individuals.

20.3 Any amendment shall enter into force and take immediate effect after it has been approved.

20.4 Any request, complaint or claim of an Individual involving this Policy shall be judged against the Policy that is in force at the time the request, complaint or claim is made.

INTERPRETATIONS AND DEFINITIONS

INTERPRETATIONS OF THIS POLICY

(a) Unless the context requires otherwise, all references to a particular Article or Annex are references to that Article or Annex in or to this document, as they may be amended from time to time;

(b) headings are included for convenience only and are not to be used in construing any provision of this Policy;

(c) if a word or phrase is defined, its other grammatical forms have a corresponding meaning;

(d) the male form shall include the female form;

(e) the words "include", "includes" and "including" and any words following them shall be construed without limitation to the generality of any preceding words or concepts and vice versa;

(f) a reference to a document (including, without limitation, a reference to this Policy) is to the document as amended, varied, supplemented or replaced, except to the extent prohibited by this Policy or that other document; and

(g) a reference to law includes any regulatory requirement, sectorial recommendation, and best practice issued by relevant national and international supervisory authorities or other bodies.

DEFINITIONS

(a) Adequacy Decision
ADEQUACY DECISION shall mean a decision issued by the European Commission under Article 25 of the EU Data Protection Directive (Directive 95/46/EC of the European Parliament) that a country or region outside the European Economic Area or a category of recipients in such country or region is deemed to provide an 'adequate' level of data protection.

(b) Archive
ARCHIVE shall mean a collection of Personal Data that are no longer necessary to achieve the purposes for which the Data originally were collected or that are no longer used for general business activities, but are used only for historical, scientific or statistical purposes, dispute resolution, investigations or general archiving purposes. An archive includes any data set that can no longer be accessed by any Employee other than the system administrator.

(c) Article
ARTICLE shall mean an article in this Policy.

(d) Business Contact Data
BUSINESS CONTACT DATA shall mean any data typically found on a business card and used by the Employee or Individual in his contact with the Company.

(e) Business Partner
BUSINESS PARTNER shall mean any Third Party, other than a Customer or Supplier, that has or had a business relationship or strategic alliance with the Company (e.g. joint marketing partner, joint venture or joint development partner).

(f) Business Purpose
BUSINESS PURPOSE shall mean a purpose for Processing Personal Data as specified in Article 2 or Article 3 or for Processing Sensitive Data as specified in Article 3 or Article 4.

(g) Children
CHILDREN shall mean individuals under the age of 13 years.

(h) Customer
CUSTOMER shall mean any person, private organization, or government body that purchases, may purchase or has purchased the Company's product or service.

(i) Data Administrator
DATA ADMINISTRATOR shall mean a person or organisation that processes data.

(j) Data Controller
DATA CONTROLLER shall mean 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

(k) Data Protection (Privacy) Officer
DATA PROTECTION (PRIVACY) OFFICER shall mean the privacy officers appointed pursuant to Articles 13.1.

(l) Data Security Breach
DATA SECURITY BREACH shall mean the unauthorized acquisition, access, use or disclosure of unencrypted Personal Data that compromises the security or privacy of such information to the extent the compromise poses a high risk of financial, reputational, or other harm to the Employee or Individual. A Data Security Breach is deemed not to have occurred where there has been an unintentional acquisition, access or use of unencrypted Personal Data by an Employee of the Company or Third Party Processor or an individual acting under their respective authority, if:

(i) the acquisition, access, or use of Personal Data was made in good faith and within the course and scope of the employment or professional relationship of such employee or other individual; and

(ii) the Personal Data are not further acquired, accessed, used or disclosed by any person.

(m) Effective Date

EFFECTIVE DATE shall mean the date on which this Policy becomes effective as set forth in Article 1.6.

(n) Employee

EMPLOYEE shall mean the following persons:

(a) an employee, job applicant or former employee of the Company including temporary workers working under the direct supervision of the Company (e.g. independent contractors and trainees). This term does not include people working in the Company as consultants or employees of Third Parties providing services to the Company;

(b) a (former) executive or non-executive director of the Company.

(o) Employee Data

EMPLOYEE DATA shall mean any information relating to an identified or identifiable Employee in the context of their employment relationship with the Company. This definition does not cover the processing of Employee Data in the Employee's capacity as a customer of the Company.

(p) Employment-at-will

EMPLOYMENT-AT-WILL means an employment relationship in which either the employer or employee can terminate the employment relationship at any time for any reason, with or without advance notice.

(q) HEINEKEN Code of Business Conduct

HEINEKEN CODE OF BUSINESS CONDUCT shall mean the HEINEKEN Code of Business Conduct as published on the HEINEKEN intranet and any amendments thereto from time to time.

(r) Individual

INDIVIDUAL shall mean any individual (employee of or any person working for) Customer, Supplier or Business Partner and any other individual whose Personal Data the Company processes in the context of the provision of its services.

(s) Management team

MANAGEMENT TEAM shall mean the Executive Committee of the Company.

(t) Original Purpose

ORIGINAL PURPOSE shall mean the purpose for which Personal Data was originally collected.

(u) Overriding Interest

OVERRIDING INTEREST shall mean the pressing interests set forth in Article 12.1 based on which the obligations of the Company or rights of Individuals set forth in Article 12.2 and 12.3 may, under specific circumstances, be overridden if this pressing interest outweighs the interest of the Employee or Individual.

(v) Personal Data or Data

PERSONAL DATA or DATA shall mean any information relating to an identified or identifiable Natural Person('data subject') 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.

(w) Policy

POLICY shall mean this Data Protection Policy for Employees, Customer, Supplier and Business Partner Data and any amendments thereto.

(x) Processing

Processing shall mean any operation that is performed on Personal Data, whether or not by automatic means, such as collection, recording, storage, organization, alteration, use, disclosure (including the granting of remote access), transmission or deletion of Personal Data.

(y) Processor Contract

PROCESSOR CONTRACT shall mean any contract for the Processing of Personal Data entered into by the Company and a Third Party Processor

(z) Responsible Managers

RESPONSIBLE MANAGER shall mean the Management Team of Champion Breweries Plc.

(aa) Secondary Purpose

SECONDARY PURPOSE shall mean any purpose other than the Original Purpose for which Personal Data is further Processed.

(bb) Sensitive Data

SENSITIVE DATA shall mean Personal Data that reveals an Individual's racial or ethnic origin, political opinions or membership in political parties or similar organizations, religious or philosophical beliefs, membership in a professional or trade organization or union, physical or mental health including any opinion thereof, disabilities, genetic code, addictions, sex life, criminal offenses, criminal records, biometric data, proceedings with regard to criminal or unlawful behaviour, social security numbers issued by the government, or any other sensitive personal information.

(cc) Staff

STAFF shall mean all Employees and other persons who Process Personal Data as part of their respective duties or responsibilities using the Company's information technology systems or working primarily from the Company's premises.

(dd) Supplier

SUPPLIER shall mean any Third Party that provides goods or services to the Company (e.g. an agent, consultant or vendor).

(ee) Third Party

THIRD PARTY shall mean any natural or legal person, public / government authority, establishment or any other body other than the Company, the Data Controller, the Data Administrator and the persons who are engaged by the Data Controller or the Data Administrator to process personal data.

(ff) Third Party Controller

THIRD PARTY CONTROLLER shall mean a Third Party that Processes Personal Data and determines the purposes and means of the Processing.

(gg) Third Party Processor

THIRD PARTY PROCESSOR shall mean a Third Party that Processes Personal Data on behalf of the Company that is not under the direct authority of the Company.