CONSOLIDATED HALLMARK HOLDINGS PLC AND SUBSIDIARIES

DATA PROTECTION POLICY

APPROVAL

Title	Consolidated Hallmark Holdings Plc Data Protection Policy		
Date Created	July 4, 2024		
	Title	**Signature**	**Date**
Prepared by:	Legal, Compliance and Secretariat		July 4, 2024
Reviewed by:	Head, Audit and Risk Management		July 8, 2024
Reviewed by:	Group Managing Director		July 15, 2024
Approved by:	Chairman, Board Governance, Nomination, and Remuneration Committee		July 22, 2024
Approved by:	Chairman, Board of Directors		July 30, 2024
Version			

1. DEFINITIONS

"Automated Decision-Making" means when a decision is made which is based solely on automated Processing (including Profiling) which produces legal effects or significantly affects an individual.;

"Consent" means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her;

"CHH" or **"Company"** means Consolidated Hallmark Holdings Plc and in this Policy, includes its Subsidiaries;

"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;

"Data Subject" means an identifiable person; one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.

"Data Protection Impact Assessment or DPIA" means tools and assessments used to identify and reduce risks of a data Processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data;

"Data Protection Laws" means the Nigeria Data Protection Act (NDPA), Nigeria Data Protection Regulation 2019 (NDPR), the General Data Protection Regulation 2018 (GDPR) (where applicable to processing carried out by the CHH) and any relevant data protection laws;

"Data Protection Officer (DPO)" means the person appointed by the company as such under the Data Protection Laws and in accordance with its requirements. A DPO is responsible for advising CHH (including its employees) on their obligations under Data Protection Laws, for monitoring compliance with Data Protection Laws, as well as with the Company's polices and providing advice.

"GDPR" means the EU General Data Protection Rules 2016/679;

"NDPR" means Nigeria Data Protection Regulation 2019;

"NDPC" means Nigeria Data Protection Commission;

"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 Media Access Control (MAC) address, Internet Protocol (IP) address, International Mobile Equipment Identity (IMEI) number, International Mobile Subscriber Identity (IMSI) number, Subscriber Identification Module (SIM) and others;

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Datatransmitted, stored or otherwise processed;

"Policy" means this Data Protection Policy;

"Privacy by Design and Default" means implementing appropriate technical and organizational measures in an effective manner to ensure compliance with the NDPR;

"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;

"Profiling" means any form of automated Processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyze or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of automated processing;

"Pseudonymisation" means replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure;

"Sensitive Personal Data" means a Data relating to religious or other beliefs, sexual tendencies, health, race, ethnicity, political views trades union membership, criminal records or any other sensitive personal information;

"Subsidiaries" means companies in which CHH has a majority shareholding of over 50%; and

"Third Party" means any natural or legal person, public authority, establishment or any other body other than the Data Subject, the Data Controller, the Data Administrator and the persons who are engaged by the Data Controller or the Data Administrator to process Personal Data.

2. INTRODUCTION

2.1 CHH takes its responsibilities regarding the management of the requirements of the Data Protection Laws very seriously. This Policy sets out how CHH manages these responsibilities.

2.2 CHH obtains, uses, stores and otherwise processes Personal Data relating to potential employees (applicants) and clients, current employees and clients, former employees and clients, current and former workers, dealers, contractors, consultants, website users and contacts, collectively referred to in this Policy as Data Subjects. When Processing Personal Data,the Company is obliged to fulfil individuals' reasonable expectations of privacy by complying with the Data Protection Laws.

2.3 This Policy therefore seeks to ensure that CHH:

a. is clear about how Personal Data must be processed and the Company's minimum standards for all those who process Personal Data on its behalf;

b. complies with the Data Protection Laws and Best Practice;

c. protects its reputation by ensuring the Personal Data entrusted to us is processed in accordance with Data Subjects' rights; and

d. protects itself from risks of Personal Data breaches and other breaches of the Data Protection Laws.

3. SCOPE

3.1 This Policy applies to all Personal Data the Company processes regardless of the location where that Personal Data is stored (e.g. on an employee's own device) and regardless of the Data Subject. All employees and others processing Personal Data on the Company's behalf must read it. A failure to comply with this Policy will result in disciplinary action.

3.2 Every Staff of CHH is required to read and assimilate the contents of this policy and to abide with it fully. CHH shall have the right to seek redress against any member of staff whose failure to comply with this policy in any manner whatsoever results in damages being sought or awarded, or any legal action instituted against the Company.

3.3 All Heads of Divisions/Departments/Units are responsible for ensuring that all CHH staff within their area of responsibility comply with this Policy and should implement appropriate practices, processes, controls and training to ensure compliance. The Heads of Divisions/Departments/Units will work closely with the Company's appointed Data Protection Officer (DPO).

3.4 The DPO of CHH shall be responsible for overseeing the implementation of this Policy.

4. PERSONAL DATA PROTECTION PRINCIPLES

4.1 When processing Personal Data, the Company shall be guided by the following principles listed below, which are set out in the Data Protection Laws.

4.2 Those principles require Personal Data to be:

a) processed lawfully, fairly, in a transparent manner and with respect for the dignity of the human person.

b) collected only for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.

c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

d) accurate and where necessary, kept up to date.

e) removed or not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the Personal Data is processed.

f) processed in a manner that ensures its security, using appropriate technical and organizational measures to protect against unauthorized or unlawful processing and against accidental loss, destruction or damage.

5. CONSENT

5.1 The Company and its representative should only obtain a Data Subject's Consent if there is no other legal basis for the processing. Consent requires genuine choice and genuine control.

5.2 A Data Subject consents to processing of his or her Personal Data if he or she clearly indicates agreement either by a statement or positive action to the Processing. Silence, pre- ticked boxes or inactivity do not mean consent. Consent must be specifically and expressly given. If Consent is given in a document that deals with other matters, such Consent must be separate and distinct from those other matters.

5.3 Consent in respect of Sensitive Personal Data must be explicit. A tick of the box would not suffice

5.4 Prior to giving Consent, the Data Subject shall be informed of his or her right and the ease to withdraw his or her Consent at any time. Withdrawal of Consent must be promptly honoured. In this instance, all further processing based on the withdrawn Consent (including processing by third parties on behalf of CHH) must cease immediately and the Data Subject shall be so notified.

5.5 Consent may need to be renewed when processing Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented, or if the Consent is historic.

5.6 The Company shall ensure that both physical and electronic records of all Consent obtained are kept so that it can demonstrate compliance.

5.7 Hard copies of Consent would be filed by the respective staff and process owner of the transaction requiring the Consent and the electronic copies should be scanned into relevant files or any subsequent document management software utilized by CHH.

5.8 No Consent shall be sought, given or accepted in any circumstance that may engender direct or indirect propagation of atrocities, hate, child rights violation, criminal acts and anti-social conducts.

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

6. DATA COLLECTION

6.1 CHH collects the following information amongst others:

- Name of Individual/Company
- Phone Number
- E-mail Address
- Contact Address
- Mailing Address
- Occupation
- Date of Birth
- Nationality
- Directors, Company Secretary and other Corporate Affairs Commission's (CAC) related Documents
- Licenses
- Next of Kin Details
- Relationship to Next of Kin
- Signatures
- Passport Photograph
- Means of Identification
- Birth certificates
- Vehicle particulars
- BVN
- PFA details /RSA Account number,
- Vendor/Supplier Registration Details, etc.
- Bank account details
- Bank Statement
- Marital Status
- Religion
- Employee's Spouse and Children Details

6.2 CHH collects the above-mentioned information through various forms, such as hard copyform, phone calls and electronic medium (e.g. email).

6.3 CHH collects the above-mentioned information for the fulfilment of her business operations and services to staff and customers.

6.4 Prior to collecting Personal Data from the Data Subject, CHH shall provide the Data Subject with its Privacy Notice, which shall, amongst others, contain the following information:

a. identity and contact details of CHH;

b. the contact details of the DPO;

c. the purpose of the Processing for which the Personal Data is intended, as well as the legal basis for the Processing;

d. the legitimate interests pursued by the Company or by any Third Party who has access to the Personal Data;

e. the recipients or categories of recipients of the Personal Data (if any);

f. where applicable, the fact that CHH intends to transfer Personal Data to a recipient in a foreign country and the existence or absence of an adequacy decision by NDPC;

g. the period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period;

h. the existence of the right to request from CHH, access to and rectification or erasure of Personal Data or restriction of Processing concerning the Data Subject or to object to Processing as well as the right to data portability;

i. the existence of the right to withdraw Consent at any time, without affecting the lawfulness of Processing based on Consent before its withdrawal;

j. the right to lodge a complaint with NDPC or any other relevant authority;

k. whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and of the possible consequences of failure to provide such data;

l. the existence of Automated Decision-Making, including Profiling and, at least, in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequence of such Processing for the Data Subject; and

m. where CHH intends to further process the Personal Data for a purpose other than that for which the Personal Data is collected, CHH shall provide the Data Subject prior to that further Processing, with information on that other purpose and any other relevant information.

6.5 The Company or its representatives must check the accuracy of any Personal Data at the point of collection and at regular intervals thereafter. All reasonable steps must be taken to destroy or amend inaccurate records without delay and out-of-date Personal Data should be updated where necessary (e.g. where it is not simply a pure historical record).

6.6 Personal Data must be accurate and, where necessary, kept up to date.

6.7 The Company shall ensure that Personal Data is recorded in the line of business application and also scanned into GIBS and/or CRM or whatever data content management solution present correct files.

6.8 Incomplete records can lead to inaccurate conclusions being drawn and in particular, where there is such a risk, the Company should ensure that relevant records are completed.

7. DATA PROCESSING

Processing shall be lawful if at least one of the following applies:

a. the Data Subject has given Consent to the Processing of his or her Personal Data for one or more specific purposes;

b. 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 the Controller 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 the controller.

f. Processing is in furtherance of the legitimate interest of CHH. Legitimate interest refers to the lawful basis of processing data including but not limited to administrative purposes (such as record keeping), provision of enhanced customer services, direct marketing (provided it is one that is reasonably envisaged by the customer), or detection of fraud. Provided always that the processing of personal data for the legitimate interest of the data controller/processor shall not override or infringe the personal interest of the data subject.

8. DATA SUBJECTS' RIGHTS

Data Subjects have rights in relation to the way CHH handles their Personal Data and include:

1. where the legal basis of CHH Processing is Consent, to withdraw that Consent at anytime;
2. to ask for access to the Personal Data that CHH holds (see below);
3. to prevent CHH use of the Personal Data for direct marketing purposes;
4. to object to CHH Processing of Personal Data in limited circumstances; and
5. to ask CHH to erase Personal Data without delay:

    a. if it is no longer necessary in relation to the purposes for which it was collected or otherwise processed;

    b. if the only legal basis of Processing is Consent and that Consent has been withdrawn and there is no other legal basis on which CHH can process that Personal Data;

    c. if the Data Subject objects to CHH Processing where the legal basis is the pursuit of a legitimate interest or the public interest and CHH can show no overriding legitimate grounds or interest; and

    d. if the Processing is unlawful.

6. to ask CHH to rectify inaccurate data or to complete incomplete data;

7. to restrict Processing in specific circumstances e.g. where there is a complaint about accuracy;

8. to ask CHH for a copy of the safeguards under which Personal Data is transferred outside of Nigeria;

9. the right not to be subject to decisions based solely on automated Processing, including profiling, except where necessary for entering into, or performing, a contract, with the Company; it is based on the Data Subject's explicit Consent and is subject to safeguards; or is authorized by law and is also subject to safeguards;

10. to prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

11. to data portability;

12. to be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedom;

13. to make a complaint to NDPC or any other regulatory body; and

14. in limited circumstances, receive or ask for their Personal Data to be transferred to a Third Party (e.g. another company which the client has dealing with) in a structured,commonly used and machine-readable format.

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

Data Subjects can exercise any of their rights by completing the CHH Data Subject Access Request (DSAR) Form and submitting to info@chhplc.com

9. REQUESTS

9.1 CHH shall take appropriate measures to provide Processing-related information to the Data Subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular, for any information addressed specifically to a child.

9.2 The information may be provided orally or in writing, or by other means, including where appropriate, by electronic means.

9.3 The identity of an individual requesting data must be verified. Where there is reasonable doubt concerning the identity of the person making the request for information, a request for the provision of additional information necessary to confirm the identity of the Data Subject may made.

9.4 Any Data Subject Access Request received must immediately be forwarded to CHH via its email address info@chhplc.com

9.5 Requests (including for Data Subject access) must be complied with, usually within one month of receipt.

9.6 The entitlement is not to documents per se (which may however be accessible by means of the Freedom of Information Act 2011, subject to any exemptions and the public interest), but to such Personal Data as is contained in the document or database.

9.7 Information provided to the Data Subject and any communication and any action taken shall be provided free of charge. Where the Data Subject's request is manifestly unfounded or excessive, in particular because of their repetitive character, CHH may either:

a. charge a reasonable fee taking into account the administrative costs of providing the information or communicating or taking the action requested; or

b. write a letter to the Data Subject stating refusal to act on the request and copy NDPC on every such occasion.

9.8 On no account shall the Company disclose Personal Data to third parties without proper authorization. For example, clients' spouses do not have an automatic right to gain access to their spouse's data. Parents of Data Subjects do not have an automatic right to gain access to their child's data.

9.9 Personal Data of Data Subjects may be disclosed to third parties in line with laid down policies and procedures of CHH and standards of regulatory authorities and regulations. CHH may share Personal Data with third parties and/or third-party service providers that complete transactions or perform services on behalf or for the benefit of the Data Subjects, in respect of:

a. Registration of staff with Pension fund administrators
b. Registration of staff with HMO providers
c. Registration of staff in compliance with any government agency requirement
d. Registration of staff with financial reporting council as may be required
e. Registration of the company with relevant government entities and corporate entities
f. Creation of data with respect to product development
g. Registration/maintenance of dealers, suppliers, customers and vendors details
h. other services which may require the processing of third-party information

9.10 Once a request is made, Personal Data shall not be altered, concealed, blocked or destroyed. The Data Protection Team/ Committee should be contacted before any changes are made to Personal Data which is the subject of an access request.

10 ACCOUNTABILITY

10.1 CHH shall implement appropriate technical and organizational measures in an effective manner to ensure compliance with the Personal Data protection principles.

The Company is responsible for, and shall demonstrate compliance with the Personal Data protection principles above.

10.2 CHH shall therefore, apply adequate resources and controls to ensure and to document the Data Protection Laws compliance including:

10.2.1 appointing a suitably qualified DPO;

10.2.2 implementing Privacy by Design when Processing Personal Data and completing a Data Protection Impact Assessment (DPIA) where Processing presents a high risk to the privacy of Data Subjects;

10.2.3 Integrating data protection into CHH procedures (in the way Personal Data is handled by the Company) and by producing required documentation such as privacy notices, records of Processing and records of Personal Data Breaches;

10.2.4 training employees and management on compliance with Data Protection Laws and keeping a record accordingly; and

10.2.5 Regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

11 DATA SECURITY

11.1 CHH is required to implement and maintain appropriate safeguards to protect Personal Data, taking into account in particular the risks to Data Subjects presented by unauthorized or unlawful Processing or accidental loss, destruction of, or damage to their Personal Data.

11.2 Safeguarding will include the use of encryption and Pseudonymisation where appropriate. It also includes protecting the confidentiality (i.e. that only those who need to know and are authorized to use Personal Data have access to it), integrity and availability of the Personal Data. The Company will regularly evaluate and test the effectiveness of those safeguards to ensure security of the Company's Processing of Personal Data.

11.3 The Company is also responsible for protecting the Personal Data processed in the course of its operation. Personal Data must be handled in a way that guards against accidental loss or disclosure or other unintended or unlawful Processing and in a way that maintains its confidentiality. Particular care must be exercised in protecting Sensitive Personal Data from loss and unauthorized access, use or disclosure.

11.4 All procedures and technologies put in place by the Company must be complied with to maintain the security of all Personal Data from the point of collection to the point of destruction.

11.5 Compliance with all applicable aspects of this Policy is mandatory. Therefore, all attempts shall be made to comply with and not circumvent the administrative, physical and technical safeguards the Company implements and maintains in accordance with the Data Protection Laws to protect Personal Data.

12 RESPONSIBILITIES OF THE DPO

The DPO is responsible for:

a. advising CHH and its staff of its obligations under the Data Protection Laws;

b. monitoring compliance with this Policy and Data Protection Laws;

c. the Company's policies with respect to data protection and monitoring, trainingand audit activities that relate to compliance with the Data Protection Laws;

d. providing advice where requested on data protection impact assessments;

e. coordinating the Company's activities in the event of a data breach incident;

f. supervising internal data processing and updating Records of Processing Activities (ROPA);

g. dealing with requests, complaints and enquiries from Data Subject and law

enforcement agencies;

h. to act as the liaison or contact person between CHH and the Company's appointed Data Protection Compliance Organization (DPCO);

i. to cooperate with and act as the contact point between CHH and NDPC; and

j. the DPO shall in the performance of his or her tasks have due regard to the risk associated with Processing operations, taking into account the nature, scope, context and purposes of Processing.

The DPO shall be a person knowledgeable in data privacy and protection related matters and shall report directly to the Company's Managing Director (or such other person as theManaging Director may designate). The DPO shall be a member of the management team of the Company, not less than the position of Senior Manager.

13 EMPLOYEE RESPONSIBILITIES

13.1 Employees who process Personal Data about employees, clients, applicants, alumni or any other individual must comply with the requirements of this Policy.

Employees must ensure that:

a. all Personal Data is kept securely;

b. no Personal Data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorized Third Party;

c. Personal Data is kept in accordance with this Policy;

d. any queries regarding data protection, including subject access requests and complaints, are promptly directed to the DPO and the Data Protection Team/ Committee.

e. any data protection breaches are swiftly brought to the attention of the Data Protection Team/ Committee and the DPO and that they support the Data Protection Team/ Committee in resolving breaches; and

f. where there is uncertainty around a data protection matter advice is sought from the Data Protection Team/ Committee and the DPO.

13.2 Where employees are responsible for ad-hoc staff or short-term staff or volunteers or contractors or interns or any person by whatever name called, doing work which involves the Processing of personal information, they must ensure that such person should have knowledge of the data protection principles.

13.3 Employees who are unsure about who are the authorized third parties to whom they can legitimately disclose Personal Data should seek advice from the Data Protection Team/ Committee or the DPO.

13.4 All staff and authorized representatives of the Company may only process Personal Data when performing their job requires it and shall not process Personal Data for any reason unrelated to their duties.

14 THIRD-PARTY DATA PROCESSORS

14.1 Data Processing by a Third Party shall be governed by a written contract between the Third Party and the Company.

14.2 Where external companies are used to process Personal Data on behalf of CHH, responsibility for the security and appropriate use of that data remains with the Company.

14.3 Where a Third-Party data processor is used:

a. the Third-Party data processor shall be chosen by CHH and the data processor must provide sufficient guarantees about its security measures to protect the Processing of Personal Data.

b. reasonable steps must be taken by the DPO to ensure that such security measures are in place.

c. a written contract establishing the type of Personal Data that will be processed and for what purpose, provided by the Data Protection Team, must be entered into by both parties i.e. the Third-Party data processor and the Company.

14.4 CHH shall ensure that the Third-Party data processor does not have a record of violating the principles of data processing and that the Third Party is accountable to NDPC or a reputable regulatory authority for data protection within or outside Nigeria.

14.5 Personal Data may be transferred to only Third-Party Service Providers (i.e. data processors) whose organizational measures comply with Data Protection Laws and who agree to act only on the Company's instructions.

14.6 For further guidance about the use of Third-Party data processors, please contact Data Protection Team/ Committee.

15. CONTRACTORS, SHORT-TERM AND VOLUNTARY STAFF

15.1 CHH is responsible for the use of Personal Data by anyone working on its behalf. Managers who employ contractors, short term or voluntary staff must ensure that they are appropriately vetted for the data they will be processing. In addition, managers should ensure that:

a. any Personal Data collected or processed in the course of work undertaken for CHH is kept securely and confidentially.

b. All Personal Data is returned to CHH on the completion of the work, including

17.4 Records of Personal Data Breaches must be kept by each employee or staff who observes or has reason to believe that a Data Breach has occurred. The record must set out:

a. the facts surrounding the breach;
b. its effects; and
c. the remedial action taken.

18 LIMITATIONS ON THE TRANSFER OF PERSONAL DATA

18.1 Where it is intended that Personal Data shall be transferred to a foreign country or to an international organisation for processing, transfer or a set of transfers of Personal Data to a foreign country or an international organisation shall take place only on one of the following conditions:

a. the Data Subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the Data Subject due to the absence of an adequacy decision and appropriate safeguards and that there are no alternatives.

b. the transfer is necessary for the performance of a contract between the Data Subject and CHH 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 CHH 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 defense of legal claims.

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.

18.4 Provided, in all circumstances above, that the Data Subject shall be 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, except where the Data Subject is answerable in duly established legal action for any civil or criminal claim in a third country.

19 RECORD KEEPING AND DATA RETENTION

19.1 The retention period of data shall be:

a. 5 (five) years after the last transaction in a contractual agreement between the Data Controller and the Data Subject;

b. Upon the presentation of evidence of death by a deceased's relative; and

c. immediately upon request by the Data Subject or his/her legal guardian where: (i) no statutory provision provides otherwise; and (ii) the Data Subject is not the subject of an investigation or suit that may require the Personal Data that is sought to be deleted.

19.2 In any other event, the Company is required to keep full and accurate records of all its data Processing activities and must keep and maintain accurate corporate records reflecting its Processing, including records of Data Subjects' Consents and procedures for obtaining Consents, where Consent is the legal basis of Processing.

19.3 These records should include, at a minimum, the name and contact details of CHH as the Data Controller and particulars of the DPO, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, Third Party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place.

19.4 When Personal Data is no longer needed for specified purposes, it shall be deleted or erased in accordance with this Policy.

19.5 Where a Data Subject has required his or her Personal Data to be rectified or erased, CHH shall inform recipients of that Personal Data that it has been erased/rectified, unless it is impossible or significantly onerous to do so. All reasonable steps shall be taken to destroy or erase from the Company's systems all Personal Data that the Company no longer requires in accordance with this Policy or any other applicable records retention policies.

20 TRAINING AND AUDIT

20.1 The Company is required to ensure that all CHH employees undergo adequate training to enable them to comply with Data Protection Laws. The Company must also regularly test its systems and processes to assess compliance.

20.2 CHH employees must undergo all mandatory data privacy related training.

20.3 CHH employees must regularly review all the systems and processes under their control to ensure they comply with this Policy.

21 DATA PRIVACY BY DESIGN AND DEFAULT AND DATA PROTECTION IMPACT ASSESSMENTS (DPIAS)

21.1 The Company is required to implement privacy-by-design measures when Processing Personal Data, by implementing appropriate technical and organizational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data-protection principles. CHH must ensure therefore that by default only Personal Data which is necessary for each specific purpose is processed. The obligation applies to the volume of Personal Data collected, the extent of the Processing, the period of storage and the accessibility of the Personal Data. In particular, by default, Personal Data should not be available to an indefinite number of persons. Strict adherence to these measures is mandatory.

23.2 Further, without a court order, the law enforcement agencies and their agents have no automatic right of access to records of Personal Data, though voluntary disclosure may be permitted for the purposes of preventing/detecting crime or for apprehending offenders. All request for Personal Data by law enforcement agents shall be referred to the DPO.

23.3 Sharing of Personal Data for research purposes may also be permissible, subject to certain safeguards.

24. CHANGES TO THIS POLICY

The Company reserves the right to change this Policy which shall be promptly communicated to concerned staff and stakeholders.

25. REVIEW OF POLICY

Subject to the final approval of the Board, this Policy shall be reviewed every 2 years or earlier if deemed necessary to ensure compliance with changing regulations or internal policy.