

GREENWICH REGISTRARS & DATA SOLUTIONS LIMITED

DATA PROTECTION POLICY

MARCH 2019

APPROVAL

The policy was reviewed and approved by

Name	Representing	Signature	Date
CHAIRMAN	BOARD DIRECTORS		14/03/19

DATA PROTECTION POLICY

APPROVAL DATE [•]

REVIEW DATE [•]

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. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not automated Processing;

"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;

"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 NDPR, the GDPR and any relevant data protection laws;

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

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

"NDPR" means Nigeria Data Protection Regulation 2019;

"NITDA" means National Information Technology Development Agency;

"Personal Data" means any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a

name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM and others;

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

"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 GDPR;

"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, behavior, 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; 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 Greenwich Registrars and Data Solutions Limited ("GRDS" or "the Company") takes its responsibilities with regard to the management of the requirements of the Data Protection Laws very seriously. This Policy sets out how GRDS manages these responsibilities.
- 2.2 GRDS obtains, uses, stores and otherwise processes Personal Data relating to potential employees (applicants) and clients, current employees and clients, former employees, shareholders, vendors and clients, current and former workers, contractors, website users and contacts, collectively referred to in this Policy as Data Subjects. When

Processing Personal Data, the Company is obliged to fulfill individuals' reasonable expectations of privacy by complying with the Data Protection Laws.

2.3 This Policy therefore seeks to ensure that GRDS:

- a. is clear about how Personal Data must be processed and the Company's expectations for all those who process Personal Data on its behalf;
- b. comply with the Data Protection Laws and with good practice;
- c. protect its reputation by ensuring the Personal Data entrusted to us is processed in accordance with Data Subjects' rights; and
- d. protect 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 member of staff of GRDS is required to read and assimilate the contents of this policy and to abide with it fully. GRDS 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 GRDS staff within their area of responsibility comply with this Policy and should implement appropriate practices, processes, controls and training to ensure compliance.
- 3.4 The DPO is responsible for overseeing this Policy. The Company DPO is Ololade Musari, he can be reached at dataprotectionofficer@gtlregistrars.com.

4. PERSONAL DATA PROTECTION PRINCIPLES

- 4.1 When you process Personal Data, you should be guided by the following principles, which are set out in the Data Protection Laws. The Company is responsible for, and must be able to demonstrate compliance with, the data protection principles listed below:
- 4.2 Those principles require Personal Data to be:
 1. processed lawfully, fairly, in a transparent manner and with respect for the dignity of the human person.

2. collected only for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.
3. adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.
4. accurate and where necessary kept up to date.
5. 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.
6. 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 You 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, you must ensure that the Consent is separate and distinct from those other matters.
- 5.3 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.
- 5.4 Consent may need to be renewed if you intend to process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented, or if the Consent is historic.
- 5.5 You will need to ensure that you have evidence of the Consent given and you should keep both physical and electronic records of all Consents obtained so that GRDS can demonstrate compliance.
- 5.6 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 M-files or any subsequent document management software utilized by GRDS.
- 5.7 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.

6. DATA COLLECTION

- 6.1 GRDS collects the following information

- Surname/Company Name
- Other name(Individual Shareholders)
- Mailing Address
- Contact Address
- E-mail Address
- G.S.M Number
- CSCS Clearing House Number
- Shareholders Account Number
- Occupation
- Nationality
- Name of Stockbroking Firm
- Next of Kin
- Relationship to Next of Kin
- Signatures
- Passport Photograph
- Means of Identification
- BVN

- 6.2 GRDS collects the above-mentioned information using a variety of hard copy forms, phone calls and electronic medium.
- 6.3 GRDS collects the above-mentioned information for the fulfilment of her Registrar and Data Solution services to customers.
- 6.4 Prior to collecting Personal Data from the Data Subject, GRDS shall provide the Data Subject with all of the following information:
- a. identity and contact details of GRDS;
 - 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 GRDS intends to transfer Personal Data to a recipient in a foreign country or a third country or international and the existence or absence of an adequacy decision by NITDA;
 - 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 GRDS, 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 NITDA 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 GRDS intends to further process the Personal Data for a purpose other than that for which the Personal Data is collected, GRDS shall provide the Data Subject prior to that further Processing, with information on that other purpose and with any relevant information.

6.5 You must check the accuracy of any Personal Data at the point of collection and at regular intervals thereafter. You must take all reasonable steps to destroy or amend inaccurate records without delay and you should update out-of-date Personal Data 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 You should ensure that Personal Data is recorded in the line of business application and also scanned into MFILES 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, you should ensure that relevant records are completed.

7. DATA PROCESSING

Ascertain that the processing of the data is lawful.

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.

8. DATA SUBJECTS' RIGHTS

Data Subjects have rights in relation to the way GRDS handles their Personal Data. These include the following rights:

- 1. where the legal basis of our Processing is Consent, to withdraw that Consent at any time;
- 2. to ask for access to the Personal Data that GRDS holds (see below);
- 3. to prevent our use of the Personal Data for direct marketing purposes;
- 4. to object to our Processing of Personal Data in limited circumstances; and
- 5. to ask us 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 GRDS can process that Personal Data;
 - c. if the Data Subject objects to our Processing where the legal basis is the pursuit of a legitimate interest or the public interest and GRDS can show no overriding legitimate grounds or interest; and
 - d. if the Processing is unlawful.
- 6. to ask us 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 us 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 authorised 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 freedoms;
13. to make a complaint to NITDA 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.

9. REQUESTS

- 9.1 GRDS shall take appropriate measures to provide any information relating to Processing to the Data Subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular, for any information addressed specifically to a child.
- 9.2 The information may be provided orally or in writing, or by other means, including where appropriate, by electronic means.
- 9.3 You must verify the identity of an individual requesting data. Where you have reasonable doubt concerning the identity of the person making the request for information, you may request the provision of additional information necessary to confirm the identity of the Data Subject.
- 9.4 You must immediately forward any Data Subject Access Request you receive to the Data Protection team/Committee at dataprotection@gtlregistrars.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, GRDS 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 NITDA on every such occasion.
- 9.8 You should not allow third parties to persuade you into disclosing Personal Data 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 GRDS and standards of regulatory authorities and regulations. GRDS 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. Dematerialization of share certificates
 - b. Updating of share register
 - c. Processing of dividend payments
 - d. Registrar Services
 - e. Probate services
 - f. Data solutions services
 - g. other services which require the processing of shareholder's information
- 9.10 You should not alter, conceal, block or destroy Personal Data once a request for access has been made. You should contact the Data Protection team/ Committee before any changes are made to Personal Data which is the subject of an access request.

10 ACCOUNTABILITY

- 10.1 GRDS must 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 must be able to demonstrate compliance with, the personal data protection principles above.
- 10.2 GRDS must, 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 our policies and procedures, in the way Personal Data is handled by us 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 GRDS 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 our Processing of Personal Data.
- 11.3 You are also responsible for protecting the Personal Data that you process in the course of your duties. You must, therefore, handle Personal Data in a way that guards against accidental loss or disclosure or other unintended or unlawful Processing and in a way that maintains its confidentiality. You must exercise particular care in protecting Sensitive Personal Data from loss and unauthorized access, use or disclosure.
- 11.4 You must comply with all procedures and technologies the Company puts in place to maintain the security of all Personal Data from the point of collection to the point of destruction.
- 11.5 You must comply with all applicable aspects of this Policy. You must, therefore, comply with and not attempt to circumvent the administrative, physical and technical safeguards the Company implements and maintains in accordance with the Data Protection Laws standards to protect Personal Data.

12 RESPONSIBILITIES OF THE DPO

The DPO is responsible for:

- a. Advising GRDS 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, training and audit activities that relate to compliance with the Data Protection Laws;
- d. providing advice where requested on data protection impact assessments;
- e. supervising internal data processing;
- f. dealing with requests, complaints and enquiries from Data Subject and law enforcement agencies;
- g. to cooperate with and act as the contact point between GRDS and NITDA; and

- h. 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.

13 EMPLOYEE RESPONSIBILITIES

- 13.1 Employees who process Personal Data about employees, shareholders, 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 You may only process Personal Data when performing your job duties requires it and you should not process Personal Data for any reason unrelated to your job 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 GRDS, 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 [GRDS] 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 what Personal Data will be processed and for what purpose, provided by the Information Compliance team, must be entered into by both parties i.e. the Third Party data processor and the Company; and
- 14.4 GRDS 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 NITDA or a reputable regulatory authority for data protection within or outside Nigeria.
- 14.5 You may only transfer Personal Data to Third Party service providers (i.e. data processors) approved by your Management and who provide sufficient guarantees to implement appropriate technical and organizational measures to 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 GRDS is responsible for the use made of Personal Data by anyone working on its behalf. Managers who employ contractors or 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 GRDS is kept securely and confidentially;
 - b. all Personal Data is returned to GRDS on the completion of the work, including any copies that may have been made. Alternatively the data is securely destroyed and GRDS receives notification in this regard from the contractor or short term / voluntary member of staff;
 - c. GRDS receives prior notification of any disclosure of Personal Data to any other organization or any person who is not a direct employee of the contractor;
 - d. any Personal Data made available by GRDS, or collected in the course of the work, is neither stored nor processed outside Nigeria unless written Consent to do so has been received from GRDS; and
 - e. all practical and reasonable steps are taken to ensure that contractors, short term or voluntary staff do not have access to any Personal Data beyond what is essential for the work to be carried out properly.

16 CLIENT AND USER RESPONSIBILITIES

Clients and Users are responsible for:

- a. familiarizing themselves with the privacy policy provided when their relationship with GRDS commences;
- b. ensuring that their Personal Data provided to GRDS is accurate and up to date.

17 REPORTING A PERSONAL DATA BREACH

- 17.1 You are required to report any Personal Data Breach where there is a risk to the rights and freedoms of the Data Subject. Where the Personal Data Breach results in a high risk to the Data Subject, he/she also has to be notified unless subsequent steps have been taken to ensure that the risk is unlikely to materialize, security measures were applied to render the Personal Data unintelligible (e.g. encryption) or it would amount to disproportionate effort to inform the Data Subject directly. In the latter circumstances, a public communication must be made or an equally effective alternative measure must be adopted to inform Data Subjects, so that they themselves can take any remedial action.
- 17.2 The Company has put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or the relevant regulator where the Company is legally required to do so. All suspected breach of Personal Data should be remedied with 1 (one) month from the date of the report of the breach.
- 17.3 If you know or suspect that a Personal Data Breach has occurred, you should immediately contact the Data Protection team/ Committee at dataprotection@gtlregistrars.com. You must retain all evidence relating to Personal Data Breaches in particular to enable GRDS maintain a record of such breaches, as required by the Data Protection Laws.
- 17.4 Records of Personal Data Breaches must be kept by each employee or member of 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.
- 17.5 GRDS will not be responsible for any Personal Data breach which occurs as a result of:
 - a. an event which is beyond the control of GRDS;
 - b. an act or threats of terrorism;
 - c. an act of God (such as, but not limited to fires, explosions, earthquakes, drought, tidal waves and floods) which compromises the Company's data protection measures;

- d. war, hostilities (whether war be declared or not), invasion, act of foreign enemies, mobilization, requisition, or embargo; and
- e. rebellion, revolution, insurrection, or military or usurped power, or civil war which compromises the Company's data protection measures.

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, the affirmation of the Attorney-General of the Federation, that the data protection levels in the foreign country or international organisation are adequate in accordance with the provisions of the NITDA regulations.
- 18.2 An application to the Attorney General of the Federation shall be accompanied by all data protection laws applicable to the foreign data processor, including all data protection policies of the said foreign recipient.
- 18.2 In the absence of any decision by the Attorney-General of the Federation as to the adequacy of safeguards in a foreign country, a 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 GRDS 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 GRDS 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.
- 18.3 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 Company is required to keep full and accurate records of all our data Processing activities. You must keep and maintain accurate corporate records reflecting our Processing, including records of Data Subjects' Consents and procedures for obtaining Consents, where Consent is the legal basis of Processing.
- 19.2 These records should include, at a minimum, the name and contact details of GRDS 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.
- 19.3 You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or erase in accordance with this Policy.
- 19.4 Where a Data Subject has required his or her Personal Data to be rectified or erased, you should inform recipients of that Personal Data that it has been erased/rectified, unless it is impossible or significantly onerous to do so. You will take all reasonable steps 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 GRDS 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 You must undergo all mandatory data privacy related training. Contact the on dataprotection@gtlregistrars.com for detailed information about the training available.
- 20.3 You must regularly review all the systems and processes under your 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. GRDS 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. You should ensure that you adhere to those measures.

- 21.2 You should ensure that your own data-handling practices default to privacy to minimize unwarranted intrusions in privacy e.g. by only disseminating Personal Data to those who need to receive it to discharge their duties.
- 21.3 GRDS must also conduct DPIAs in respect of high-risk Processing before that Processing is undertaken.
- 21.4 You should conduct a DPIA (and discuss your findings with the DPO) in the following circumstances:
 - a. the use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
 - b. automated Processing including Profiling;
 - c. large scale Processing of sensitive (special category) data; and
 - d. large scale, systematic monitoring of a publicly accessible area.
- 21.5 A DPIA must include:
 - a. a description of the Processing, its purposes and the Company's legitimate interests if appropriate;
 - b. an assessment of the necessity and proportionality of the Processing in relation to its purpose;
 - c. an assessment of the risk to individuals; and
 - d. the risk-mitigation measures in place and demonstration of compliance.

22. DIRECT MARKETING

- 22.1 The Company is subject to certain rules and privacy laws when marketing to our clients and potential clients, alumni and any other potential user of our services. The limited exception for existing clients allows organizations to send marketing texts or emails if they have obtained contact details in the course of a sale to the person they are marketing similar services to, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.
- 22.2 The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.
- 22.3 A Data Subject's objection to direct marketing must be promptly honored. If a Data Subject opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

23 SHARING PERSONAL DATA

- 23.1 In the absence of Consent, a legal obligation or other legal basis of Processing, Personal Data should not generally be disclosed to third parties unrelated to the Company.
- 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. You should refer law enforcement agents that request Personal Data to the DPO.
- 23.3 Sharing of Personal Data for research purposes may also be permissible, subject to certain safeguards. If you need guidance or clarification, please contact the Data Protection team/ Committee on dataprotection@gtlregistrars.com.

24. CHANGES TO THIS POLICY

The Company reserves the right to change this Policy at any time without notice to you so please check regularly to obtain the latest copy.