Issue date: _____

SKANESTAS INVESTMENTS LIMITED

DATA PROTECTION POLICY

1. Aim of the Data Protection Policy

1.1. As part of its social responsibility, the SKANESTAS INVESTMENTS LIMITED (hereinafter – the "Company") is committed to compliance with data protection laws. This Data Protection Policy (hereinafter – Policy) fully applies to the Company and is based on globally accepted, basic principles on data protection. Ensuring data protection is the foundation of trustworthy business relationships and the reputation of the Company as an attractive employer.

1.2. The Data Protection Policy provides one of the necessary framework conditions for domestic and cross-border data transmission among the Company. It ensures the adequate level of data protection prescribed by the European Union Data Protection Regulation and the laws of Republic of Cyprus for domestic and cross-border data transmission.

1.3. The Board of Directors and management of SKANESTAS INVESTMENTS LIMITED, located in the Republic of Cyprus, are committed to compliance with all relevant EU and Member State laws in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information the Company collects and processes in accordance with the General Data Protection Regulation (GDPR) - REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

2. Scope and amendment of the Data Protection Policy

2.1. This Data Protection Policy fully applies to the Company and is applied for the purposes of personal data processing.

2.2. The GDPR and this policy apply to all of the Company personal data processing functions, including those performed on customers', clients', employees', suppliers' and partners' personal data, and any other personal data the Company processes from any source.

2.3. This policy applies to all Employees/Staff and interested parties of the Company such as outsourced suppliers. Any breach of the GDPR or this Data Protection Policy will be dealt with under SKANESTAS INVESTMENTS LIMITED disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

2.4. Partners and any third parties working with or for SKANESTAS INVESTMENTS LIMITED, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by the

Company without having first entered into a data confidentiality agreement, which imposes on the third party obligations no less onerous than those to which the Company is committed, and which gives the Company the right to audit compliance with the agreement.

2.5. This Policy may be updated from time to time.

3. Definitions and roles under the General Data Protection Regulation

3.1. Personal data - 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;

Data controller - the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

Data subject – any living individual who is the subject of personal data held by a Company;

Processing - 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;

Processor - a natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller;

Personal data breach - 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;

Consent of the data subject - 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;

Third party - a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

3.2. The Company is a data controller and/or data processor under the GDPR.

3.3. Top Management and all those in managerial or supervisory roles throughout the Company are responsible for developing and encouraging good information handling practices within the Company; responsibilities are set out in individual job descriptions.

3.4. Data Protection Officer is responsible for reviewing the register of processing annually in the light of any changes to the Company activities (as determined by changes to the data inventory register and the management review) and to any additional requirements identified by means of data protection impact assessments. This register needs to be available on the supervisory authority's request.

3.5. Data Protection Officer is accountable to Board of Directors of the Company for the management of personal data within the Company and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:

3.5.1 development and implementation of the GDPR as required by this policy; and

3.5.2 security and risk management in relation to compliance with the policy.

3.6. Data Protection Officer, who Board of Directors considers to be suitably qualified and experienced, has been appointed to take responsibility for SKANESTAS INVESTMENTS LIMITED compliance with this policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that the Company complies with the GDPR, as do other manager's in respect of data processing that takes place within their area of responsibility.

3.7. Compliance with data protection legislation is the responsibility of all Employees/Staff of the Company who process personal data.

3.8. Employees/Staff of the Company are responsible for ensuring that any personal data about them and supplied by them to the Company is accurate and up-to-date.

4. Principles for processing personal data

4.1. Fairness and lawfulness

The individual rights of the data subjects must be protected. Personal data must be collected and processed in a legal and fair manner. Lawful – identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing", for example consent. Fairly – in order for processing to be fair, the data controller has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources.

4.2. Restriction to a specific purpose

Personal data can be processed only for the purpose that was defined before the data was collected. Subsequent changes to the purpose are only possible to a limited extent and require substantiation.

4.3. Transparency

The GDPR includes rules on giving privacy information to data subjects. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.

The specific information that must be provided to the data subject must, as a minimum, include:

4.3.1 the identity and the contact details of the controller and, if any, of the controller's representative;

4.3.2 the contact details of the Data Protection Officer;

4.3.3 the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

4.3.4 the period for which the personal data will be stored;

4.3.5 the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;

4.3.6 the categories of personal data concerned;

4.3.7 the recipients or categories of recipients of the personal data, where applicable;

4.3.8 where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;

4.3.9 any further information necessary to guarantee fair processing.

4.4. Confidentiality

Personal data is a subject to data secrecy.

Personal data can only be collected for specific, explicit and legitimate purposes. Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the supervisory authority as part of the Company register of processing.

4.5. Personal data must be adequate, relevant and limited to what is necessary for processing.

4.6. The Data Protection Officer is responsible for ensuring that the Company does not collect information that is not strictly necessary for the purpose for which it is obtained.

4.7. All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be include a fair processing statement or link to privacy statement and approved by the Data Protection Officer.

4.8. The Data Protection Officer will ensure that, on an annual basis all data collection methods are reviewed to ensure that collected data continues to be adequate, relevant and not excessive.

4.9. Personal data must be accurate and kept up to date with every effort to erase or rectify without delay.

4.10. Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

4.11. The Data Protection Officer is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

4.12. It is also the responsibility of the data subject to ensure that data held by the Company is accurate and up to date. Completion of a registration or application form by a data subject will include a statement that the data contained therein is accurate at the date of submission.

4.13. Employees/Staff/customers/others should be required to notify the Company of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of the Company to ensure that any notification regarding change of circumstances is recorded and acted upon.

4.14. The Data Protection Officer is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

4.15. On at least an annual basis, the Data Protection Officer will review the retention dates of all the personal data processed by the Company, by reference to the data inventory.

4.16. The Data Protection Officer is responsible for responding to requests for rectification from data subjects within one month. This can be extended to a further two months for complex requests. If the Company will not comply with the request, the Data Protection Officer must respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority and seek judicial remedy.

4.17. The Data Protection Officer is responsible for making appropriate arrangements that, where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.

4.18. Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

4.19. Personal data must be processed in a manner that ensures the appropriate security.

The Data Protection Officer will carry out a risk assessment taking into account all the circumstances of the Company's controlling or processing operations.

4.20. In determining appropriateness, the Data Protection Officer should also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or customers) if a security breach occurs, the effect of any security breach on the Company itself, and any likely reputational damage including the possible loss of customer trust.

4.21. When assessing appropriate technical measures, the Data Protection Officer will consider the following:

- Password protection;
- Automatic locking of idle terminals;
- Removal of access rights for USB and other memory media;
- Virus checking software and firewalls;
- Role-based access rights including those assigned to temporary staff;
- Encryption of devices that leave the organisations premises such as laptops;
- Security of local and wide area networks;
- Identifying appropriate international security standards relevant to the Company.

4.22. When assessing appropriate organisational measures the Data Protection Officer will consider the following:

- The appropriate training levels throughout the Company;
- Measures that consider the reliability of employees (such as references etc.);
- The inclusion of data protection in employment contracts;
- Identification of disciplinary action measures for data breaches;
- Monitoring of staff for compliance with relevant security standards;
- Physical access controls to electronic and paper based records;
- Adoption of a clear desk policy;
- Storing of paper based data in lockable fire-proof cabinets;
- Restricting the use of portable electronic devices outside of the workplace;
- Restricting the use of employee's own personal devices being used in the workplace;
- Adopting clear rules about passwords;
- Making regular backups of personal data and storing the media off-site;
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside.

4.23. The controller must be able to demonstrate compliance with the GDPR's other principles (accountability).

4.24. The GDPR includes provisions that promote accountability and governance. The Company will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, breach notification procedures and incident response plans.

SKANESTAS INVESTMENTS

5. Scope of data processing

5.1. Throughout the period of using the Company's services and after the termination of a contractual relationship, the Company shall be entitled to process the information, including personal data, of a data subject in compliance with the purposes set forth in Paragraph 7 of the Policy.

5.2. More precisely, data processing means obtaining, collecting, recording, photographing, audio recording, video recording, organizing, storing, altering, restoring, revoking or disclosing (including transferring and/or disclosing information to third parties who will subsequently process the data in compliance with the purposes set forth by the Policy) from the data subject or third parties for the purpose of transferring, disseminating or making available through different means, grouping or combining, blocking, erasing or destroying.

5.3. Personal data include but are not limited to:

(i) Name and surname of data subject;

(ii) Personal identity number and/or unique features of electronic identity card, number of passport;

(iii) Address of registration and/or factual residency;

(iv) Telephone/mobile phone number;

(v) E-mail address;

(vi) Credit history (negative as well as positive, including debts ongoing and/or already covered, loans and details of payment thereof) and solvency status (Solvency score of data subject, criteria and/or methodology thereof);

(vii) Immovable and movable things and features thereof, under the ownership and/or possession of data subject;

(viii) Data related to employer, as well as information related to the terms of employment (place of employment, salary, working time and so forth);

(ix) Data related to data subject's Company account(s) in the Company and other commercial companies operating in the Republic of Cyprus, including, but not limited to, outstanding balance of such accounts for a specific time and date and executed transactions on these accounts throughout specific period of time;

(x) Data disclosed while using various electronic channels and/or the internet (including but not limited to web-cookies and so forth) and activities of data subject and/or third parties indicated by data subject while using abovementioned channels (including but not limited to authentication into such channels and actions executed or transaction history);

(xi) Data related to family member, relative and other persons residing at data subject's address of factual residency.

(xii) Any other type of data related to the Client, which enables to identify and/or characterize, and/or group the data subject by his/her physical, physiological, psychological, economic, cultural or social qualities, by using transactional activities listed, or referred to above.

5.4. In case the data subject, for the purpose of using the Company's service, provides the Company with information (including but not limited to personal data, solvency, property (asset) status and so forth) related to the third parties (additional card holder, guarantor, family members, employer and so forth) and the Company processes such information, including personal data, for the purposes of performing Company services and/or marketing, the data subject is held personally responsible for obtaining the consent of any such third party on processing their respective personal data by the Company. When the data subject provides the Company (or its authorized personnel) with such information, it is presumed that the data subject has obtained their respective consent and the Company is not further required to obtain such consent by itself. The data subject is personally responsible for any damage/loss, which may occur to the Company by the data subject's failure to comply with or under-perform the obligation to obtain the consent of third parties.

6. Data subjects' rights

6.1. Data subjects have the following rights regarding data processing, and the data that is recorded about them:

6.1.1 To make subject access requests regarding the nature of information held and to whom it has been disclosed.

6.1.2 To prevent processing likely to cause damage or distress.

6.1.3 To prevent processing for purposes of direct marketing.

6.1.4 To be informed about the mechanics of automated decision-taking process that will significantly affect them.

6.1.5 To not have significant decisions that will affect them taken solely by automated process.

6.1.6 To sue for compensation if they suffer damage by any contravention of the GDPR.

6.1.7 To take action to rectify, block, erase, including the right to be forgotten, or destroy inaccurate data.

6.1.8 To request the supervisory authority to assess whether any provision of the GDPR has been contravened.

6.1.9 To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.

6.1.10 To object to any automated profiling that is occurring without consent.

6.2 The Company ensures that data subjects may exercise these rights:

6.2.1 Data subjects may make data access requests; this procedure also describes how the Company will ensure that its response to the data access request complies with the requirements of the GDPR.

6.2.2 Data subjects have the right to complain to the Company related to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled in line with the complaints procedure.

7. Purposes of data processing

7.1. The Company may process personal data of the data subject or third parties indicated by the data subject for various purposes including but not limited to:

(i) Duly performance of Company services;

(ii) Cases determined by the legislation;

(iii) Optimizing and developing the Company's services during which the Company analyses the data of a data subject related to Client orders;

(iv) Preparation and presentation of reports;

(v) Prevention of fraud, money laundering or other criminal activities.

8. Processing data of applicants or employees

8.1. The Company is entitled to processing subject's personal data which was disclosed for the purpose of considering an initiation of employment and/or internship of such a person (hereinafter – Applicant). If the applicant is rejected, failed to proceed through selection process, unsuccessfully ended the trial period, his/her data must be deleted, unless the applicant has agreed (by electronic as well as non-electronic means) to remain on file for a future selection process by the Company and/or third parties.

8.2. If it should be necessary during the application procedure to collect information on an applicant from a third party, the requirements of data protection laws have to be observed.

8.3. There must be legal authorization to process personal data that is related to the employment relationship but was not originally part of performance of the employment agreement. This can include: a) legal requirements, b) consent of the applicant (by electronic as well as non-

electronic means) or c) the legitimate interest of the Company or third party and d) purposes set forth in Paragraph 7 of the Policy.

9. Processing of highly sensitive data

9.1. Highly sensitive personal data can be processed only under applicant's (data subject) written consent or without such consent when processing is expressly permitted or prescribed under national law (including but not limited to considering an initiation of employment). Highly sensitive data is data about racial and ethnic origin, political beliefs, religious or philosophical beliefs, union membership, health and sexual life, criminal record, administrative detention, preventive measures, plea bargain, diversion, recognition as a victim or an affected by the crime, as well as biometric and genetic data, which enable the identification of a physical person.

9.2. Applicants consent on processing highly sensitive personal data must be clearly expressed.

10. Consent

10.1 The Company understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.

10.2 The Company understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

10.3 There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication. The Controller must be able to demonstrate that consent was obtained for the processing operation.

10.4 For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

10.5 In most instances, consent to process personal and sensitive data is obtained routinely by Company using standard consent documents e.g. when a new client signs a contract, or during induction for participants on programmes.

SKANESTAS INVESTMENTS

11. Security of data

11.1 All Employees/Staff are responsible for ensuring that any personal data that the Company holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by the Company to receive that information and has entered into a confidentiality agreement.

11.2 All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Access Control Policy. All personal data should be treated with the highest security and must be kept:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerised, password protected in line with corporate requirements in the Access Control Policy; and/or
- stored on (removable) computer media.

11.3 Care must be taken to ensure that PC screens and terminals are not visible except to authorised Employees/Staff of the Company.

11.4 Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit authorisation. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving in line with retention policy.

11.5 Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'.

12. Disclosure of data

12.1 The Company must ensure that personal data is not disclosed to unauthorised third parties, which includes family members, friends, government bodies, and in certain circumstances, the Police. All Employees/Staff should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of the Company business.

12.2 All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Officer.

13. Retention and disposal of data

13.1 The Company shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

13.2 The Company may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

13.3 The retention period for each category of personal data will be set out along with the criteria used to determine this period including any statutory obligations the Company has to retain the data.

13.4 The Company data retention and data disposal procedures will apply in all cases.

13.5 Personal data must be disposed of securely in accordance with the principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects. Any disposal of data will be done in accordance with the secure disposal procedure.

14. Data transfers

14.1 All exports of data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the GDPR as 'third countries') are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects".

The transfer of personal data outside of the EEA is prohibited unless one or more of the specified safeguards, or exceptions, apply:

14.1.1 An adequacy decision

The European Commission can and does assess third countries, a territory and/or specific sectors within third countries to assess whether there is an appropriate level of protection for the rights and freedoms of natural persons. In these instances no authorisation is required.

Countries that are members of the European Economic Area (EEA) but not of the EU are accepted as having met the conditions for an adequacy decision.

A list of countries that currently satisfy the adequacy requirements of the Commission are published in the *Official Journal of the European Union. http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm*

14.1.2 Binding corporate rules

The Company may adopt approved binding corporate rules for the transfer of data outside the EU. This requires submission to the relevant supervisory authority for approval of the rules that the Company is seeking to rely upon.

14.1.3 Model contract clauses

The Company may adopt approved model contract clauses for the transfer of data outside of the EEA.

14.1.4 Exceptions

In the absence of an adequacy decision, binding corporate rules and/or model contract clauses, a transfer of personal data to a third country or international organisation shall only take place on one of the following conditions:

 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;

 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;

 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;

 the transfer is necessary for important reasons of public interest;

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

 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.

15. Information asset register/data inventory

15.1 The Company has established a data inventory and data flow process as part of its approach to address risks and opportunities throughout its GDPR compliance project. The Company's data inventory and data flow determines:

 business processes that use personal data;
 source of personal data;
 volume of data subjects;
 description of each item of personal data;
 processing activity;
 maintains the inventory of data categories of personal data processed;
 documents the purpose(s) for which each category of personal data is used;
 recipients, and potential recipients, of the personal data;
 the role of the Company throughout the data flow;
 key systems and repositories;
 any data transfers; and
 all retention and disposal requirements.

15.2 The Company is aware of any risks associated with the processing of particular types of personal data.

15.2.1 The Company assesses the level of risk to individuals associated with the processing of their personal data.

15.2.2 The Company shall manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

15.2.3 The Data Protection Officer shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the supervisory authority.

15.2.4 Appropriate controls will be selected and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to the Company's documented risk acceptance criteria and the requirements of the GDPR.

16. Audio recording

16.1. The data subject should be informed of audio-recording in advance.

17. Data protection control

17.1. Compliance with this Data Protection Policy and the applicable data protection laws is checked regularly by Data Protection Officer. The responsible data protection authority can perform its own controls of compliance of the Company with the regulations of this Policy, as permitted under national law.

Appendix – Consent of the Data Subject.

(Sign):_____

Date: _____