DATA PROTECTION AND PRIVACY POLICY – CONTROLLER – PROCESSOR

1. SCOPE

a. **Centralspot Trading Ltd**., a limited liability company incorporated under the laws of the Republic of Cyprus bearing registration number HE 325259 having its registered office at 116, Gladstonos Street, M. Kyprianou House, Floor 3&4, 3032 Limassol, Cyprus, a Cyprus Investment Firm authorized and regulated by the Cyprus Securities Exchange Commission (CySEC) with license number 238/14 or its Affiliates (the "**Company**" and/or the "**Controller**") and the Partner (the "**Processor**") are parties to the Agreement (each the "**Party**"), to which this Policy applies. If the Partner Processes Personal Data, or if the Partner has access to Personal Data in the course of its performance under the Agreement, the Partner shall comply with the terms and conditions of this Data Protection and Privacy Policy (the "**Policy**")

b. This Data Protection may include the Standard Contractual Clauses and related Exhibits (the "**Attachments**"). Subject to the Parties' obligations in relation to the General Data Protection Regulation 2016/679, the Parties wish to set out the terms of the Data Protection Agreement in order to ensure that their obligations relating to the processing of personal data is subject to the provisions of the GDPR. By accepting this Policy, the Partner shall qualify as the Data Processor, as this term is defined under the Data Protection Laws.

2. DEFINITIONS

All capitalized terms not defined in this Policy shall have the meanings set forth in the Agreement.

a. "**Affiliate**" means any person or entity directly or indirectly controlling, controlled by, or under common control with a Party. For the purpose of this definition, "control" (including, with correlative meanings, the terms "controlling", "controlled by" and "under common control with") means the power to manage or direct the affairs of the person or entity in question, whether by ownership of voting securities, by contract or otherwise;

b. "**Affiliate Agreement**" means the agreement between the Company and the Partner which involves the Partner having access to or otherwise Processing Personal Data;

c. "**Approved Jurisdiction**" means a member state of the EEA, or other jurisdiction as may be approved as having adequate legal protections for data by the European Commission;

d. "**Breach Incident**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;

e. "**Data Protection Laws**" means any and/or all applicable domestic and foreign laws, rules, directives and regulations, on any local, provincial, state or deferral or national level, pertaining to data privacy, data security and/or the protection of Personal Data, including the General Data Protection Regulation 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 (the "**GDPR**") and the Privacy and Electronic Communications Directive 2002/58/EC (and respective local implementing laws) concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), including any amendments or replacements to them;

f. **"EEA**" means those countries that are members of the European Economic Area;

g. **"Partner**" refers to the legal entity, regardless of the form of organization, identified in the Agreement;

h. "**Personal Data**" or "**personal data**" means any information that is about, or can be related to, an identifiable individual. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual, natural person. Personal Data shall be considered Confidential Information regardless of the source;

i. **"Process**" or "**process**" means any operation or set of operations that is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, access to, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction. **"Processes**" or "**processes**" and "**Processing**" or "**processing**" shall be construed accordingly;

j. "**Special Categories of Data**" means personal data that requires an extra level of protection and a higher duty of care under Data Protection Laws, for example, information on medical or health conditions, certain financial information, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual preferences, or information related to offenses or criminal convictions.

3. DATA PROTECTION AND PRIVACY

a. If Partner has access to or otherwise Processes Personal Data, then Partner shall:

i. Only Process the Personal Data in accordance with Company's documented instructions and on its behalf, and in accordance with the Agreement and this Policy and related Attachments unless required to process that Personal Data for other purposes by EU Law. Where such a requirement is placed on the Partner it shall provide prior notice to the Company unless EU Law prohibits the giving of notice on important grounds of public interest. This notice must be sent to partners@fxvc.eu

ii. Promptly inform the Company if, in its opinion, the Company's instructions would be in breach of Data Protection Laws;

iii. Take reasonable steps to ensure the reliability of its staff and any other person acting under its supervision who may come into contact with, or otherwise have access to and Process, Personal Data; ensure persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; and ensure that such personnel are aware of their responsibilities under this Policy and any Data Protection Laws (or Partner's own written binding policies are at least as restrictive as this Policy);

iv. Provide reasonable assistance to the Company, and at the Company's request, any other service provider that assists the Company in complying with Data Protection Laws, to conduct a privacy impact assessment (and any related consultations) where required under Data Protection Laws;

v. Assist Company as needed to cooperate with and respond to requests from supervisor authorities, data subjects, customers, or others to provide information (including details of the services provided by Partner) related to Partner's Processing of Personal Data;

vi. Notify the Company immediately and without undue delay, and no later than twenty-four (24) hours, should it become aware of a Breach Incident. The notification must be sent to partners@fxvc.eu . As part of that notification, the Partner shall provide:
   a. a description of the nature of the Breach Incident, including the volume and type of Personal Data affected and the categories and number of individuals concerned;
   b. the likely consequences of the Breach Incident; and
   c. a description of the measures taken or proposed to be taken to address the Breach Incident, including measures to mitigate any possible adverse effects;

vii. Provide full, reasonable cooperation and assistance to Company in:
   a. Allowing data subjects to exercise their rights under the Data Protection Laws, including (without limitation) the right of access, right to rectification, restriction of Processing, erasure, data portability, object to the Processing, or the right not to be subject to an automated individual decision making;
   b. Ensuring compliance with any notification obligations of personal data breach to the supervisory authority and communication obligations to data subjects, as required under Data Protection Laws;
   c. Ensuring compliance with its obligation to carry out data protection impact assessments with respect to the Processing of Personal Data, and with its prior consultation with the supervisory authority obligation (as applicable).

viii. Only process or use Personal Data on its systems or facilities to the extent necessary to perform its obligations under the Agreement;

ix. As required under Data Protection Laws, maintain accurate written records of any and all the Processing activities of any Personal Data carried out under the Agreement (including the categories of Processing carried out and, where applicable, the transfers of Personal Data), and shall make such records available to the applicable supervisory authority on request;

x. Make all reasonable efforts to ensure that Personal Data are accurate and up to date at all times while in its custody or under its control, to the extent Partner has the ability to do so;

xi. Not lease, sell or otherwise distribute Personal Data;

xii. Promptly notify the Company of any investigation, litigation, arbitrated matter or other dispute relating to Partner's information security or privacy practices as it relates to the Processing of Personal Data;

xiii. Promptly notify Company in writing and provide Company an opportunity to intervene in any judicial or administrative process if Partner is required by law, court order, warrant, subpoena, or other legal or judicial process to disclose any Personal Data to any person other than Company;

xiv. Promptly notify the Company if it receives a request from an individual attempting to exercise their rights under the Data Protection Laws. This notification must be sent to partners@fxvc.eu . The Partner shall act in accordance with the Company's reasonable instructions when dealing with that request; and

xv. Upon termination of the Agreement, or upon Company's written request at any time during the term of the Agreement, Partner shall cease to Process any Personal Data received from Company, and within a reasonable period will at the request of Company: (1) return the Personal Data; or (2) securely and completely destroy or erase all Personal Data in its possession or control (including any copies thereof), unless and solely to the extent the foregoing conflicts with any applicable laws. At Company's request, Partner shall give Company a certificate confirming that it has fully complied with this clause.

b. The Parties will each comply with the GDPR and the Data Protection Laws when performing their obligations under the Policy.

c. The Partner shall implement appropriate technical and organisational measures to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access. This shall include:

i. ensuring any of its employees or agents or other persons to whom it provides access to Personal Data are obliged to keep it confidential;

ii. the use of pseudonymisation and encryption of Personal Data, where appropriate;

iii. measures to ensure the ongoing confidentiality, integrity, availability and resilience of the Processor's systems and services;

iv. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;

v. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing of Personal Data; and

vi. assisting the Company to comply with its own data security obligations under Data Protection Laws.

d. The Partner shall not transfer Personal Data to a country outside of the EEA that has not received a binding adequacy decision from the EU Commission pursuant to Article 45 GDPR without obtaining the Company's consent and taking such measures as the Company may reasonably specify to ensure the transfer complies with Data Protection Laws including, at the Company's request, entering into (or procuring that such other persons as the Company may reasonably specify enter into) standard contractual clauses with the Company (or such other person as the Company may reasonably specify) in the form approved by the EU Commission.

e. At the request of the Company, the Partner shall provide evidence of its compliance with this Policy and allow the Company to audit that compliance (either itself or by using an auditor nominated by the Company).

f. The Company uses your' personal information only as required to provide quality service and security to its Affiliates/Partners. This information helps the Company to improve its services, customize browsing experience and enables it to inform its Affiliates/Partners of additional, products, services or promotions relevant to Affiliates/Partners provided that have consented to the usage of this data for such purposes.

g. It shall be noted that the Company may anonymize or de-identify the collected information which, on its own, cannot personally identify you. In addition, the combination of Personal and non-Personal information is considered as Personal information and will be treated so while remaining combined.

h. The Company may disclose your Personal Data if it is under a duty to disclose or share your personal data and transaction data in order to comply with any legal obligation, or in order to enforce or apply the terms and conditions of the Affiliated Agreement; or to protect the rights, property, or safety of the Company, our customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

i. In the event that that the Company sell or buy any business or assets, it may disclose your personal data and transaction data to the prospective seller or buyer of such business or assets. If substantially all of the assets of the Company are acquired by a third party, personal data and transaction data held by it about its customers will be one of the transferred assets;

j. We will use all reasonable endeavours to ensure that any companies to whom we disclose your confidential information is compliant with the GDPR (or an equivalent standard) as regards its use and storage of your Personal Data.

k. The Company respects your privacy rights and provides you with reasonable access to the Personal Data that you may have provided through your use of the Services. Your principal rights under the GDPR are as follows:

   i. the right for information;
   ii. the right to access;
   iii. the right to rectification;
   iv. the right to erasure; the right to be forgotten;
   v. the right to restrict processing;
   vi. the right to object to processing;
   vii. the right to data portability;
   viii. the right to withdraw consent;

l. You shall have the right to exercise any of those rights, as long as such requests do not conflict with the laws of the Republic of Cyprus.

m. If you want to exercise any of those rights or have any enquiries, you should contact our Data Protection Officer (DPO) through the contact information via email to dpo-support@kpklegal.com

The Company shall try to respond to all requests within 14 calendar days. Please note that it may take us longer than 14 calendar days if your request is particularly complex or you have made a number of requests. In this case, we will notify you within 14 (fourteen) calendar days of the

receipt of your request and keep you updated.

If you are not satisfied with our response to your complaint, you have the right to lodge a complaint with the Cyprus' Data Protection Authority.

You can find details about how to do this on the following website:

http://www.dataprotection.gov.cy

n. You should put your request in written with your own words and send it to the DPO by e-mail. We will acknowledge your request within seventy-two (72) hours and handle it promptly. We are going to process and reply to your request within a month, with a possibility to extend this period for particularly complex requests in accordance with Applicable Law. We will retain your Personal Data for as long as your account is active, as needed to provide you services, or to comply with our legal obligations, resolve disputes and enforce our agreements.

You have the right to lodge a complaint with a supervisory authority which is the Commission for personal data protection in Cyprus you may exercise through the contact information listed below:

DATA COMMISSIONER OF THE REPUBLIC OF CYPRUS
Address: 1 Iasonos str., 1082 Nicosia
P.O.Box 23378, 1682 Nicosia
+357 22818456
+357 22304565
commissioner @dataprotection.gov.cy (w)
http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/home_en/home_en?opendocument

4. SUBCONTRACTING

a. Subject to paragraph 4.b. below, Partner shall not subcontract its obligations under this Policy to another person or entity (the "**Contractor(s)**"), in whole or in part, without Company's prior written approval or general written authorization, and shall inform the Company of any intended changes concerning the addition/replacement of other processors;

b. The Company provides the Partner with a general authorisation to engage other processors to process Personal Data where such other processors are not engaged solely for the purpose of this Policy and the products and/or services provided by such other processors do not constitute a material component of the products and/or services provided under the Policy ("**Non-Material Sub-processors**"). The Partner shall provide the Company with a list of the Non-Material Sub-processors as soon as reasonably possible (and in any event no later than 30 days from their engagement). The Partner shall also give the Company prior notice of any intended addition to, or replacement of, those Non-Material Sub-processors. If the Company reasonably objects to that change, the Partner shall refrain from making that addition or replacement.

c. Partner will execute a written agreement with such approved Contractor (including Non-Material Sub-processors) it engages to process Personal Data, in accordance with this Policy, containing equivalent terms to this Policy and the applicable Attachments (provided that Partner shall not be entitled to permit the Contractor to further sub-contract or otherwise delegate all or any part of the Contractor's processing without Company's prior written consent at Company's sole discretion)

and which expressly provides Company with third party beneficiary rights to enforce such terms and/or require Partner to procure that the Contractor enters into a Data Protection agreement with Company directly. That contract must impose obligations on the processor equivalent to those set out in this Policy and the Partner shall ensure the other processor complies with those obligations. Where the other processor fails to comply with those obligations, the Partner shall remain liable to the Company for such failure.

d. Partner shall have a written security policy that provides guidance to its Contractors to ensure the security, confidentiality, integrity and availability of Personal Data and systems maintained or processed by Partner.

e. Company may require Partner to provide Company with full details of the proposed Contractor's involvement including but not limited to the identity of the Contractor, its data security record, the location of its processing facilities and a description of the access to Personal Data proposed.

f. Partner shall be responsible for the acts or omissions of Contractors to the same extent it is responsible for its own actions or omissions under this Policy.

g. The Company is not responsible for the privacy policies or the content of sites to which http://www.fxvcpartners.com appears and has not control of the use or protection of information provided by the Affiliates / Partners or collected by those sites.

5. THE TRANSFER OF PERSONAL DATA

a. If the Partner is required to transfer Personal Data to a third country or an international organization under applicable laws, it shall inform the Company of that legal requirement before processing. If, subject to Company's prior consent, Partner Processes Personal Data from the EEA in a jurisdiction that is not an Approved Jurisdiction, Partner shall ensure that it has a legally approved mechanism in place to allow for the international data transfer. If Partner intends to rely on Standard Contractual Clauses, the following additional terms will apply to Partner and Partner's partners and/or affiliates (where subcontracting or performance is allowed by the Agreement):

   i. The Standard Contractual Clauses set forth in the Attachments will apply. If such Standard Contractual Clauses are superseded by new or modified Standard Contractual Clauses, the new or modified Standard Contractual Clauses shall be deemed to be incorporated into this Policy, will replace the then-current Attachments, and Partner will promptly begin complying with such Standard Contractual Clauses. Partner will abide by the obligations set forth under the Standard Contractual Clauses for data importer and/or sub-processor as the case may be.

   ii. The Adequacy decisions set forth in the Attachments will apply. If such Adequacy decisions are superseded by new or modified Adequacy decisions, the new or modified Adequacy decisions shall be deemed to be incorporated into this Policy, will replace the then-current Attachments, and Partner will promptly begin complying with such Adequacy decisions. Partner will abide by the obligations set forth under the Adequacy decisions for data importer and/or sub-processor as the case may be.

   iii. The Binding Corporate Rules (BCR) set forth in the Attachments will apply. If such Binding Corporate Rules (BCR) are superseded by new or modified Binding Corporate Rules (BCR), the new or modified Binding Corporate Rules (BCR) shall be deemed to be incorporated into

this Policy, will replace the then-current Attachments, and Partner will promptly begin complying with such Binding Corporate Rules (BCR). Partner will abide by the obligations set forth under the Binding Corporate Rules (BCR)for data importer and/or sub-processor as the case may be.

iv. If Partner subcontracts any Processing of Personal Data (as allowed by the Agreement and Applicable Law), it will:
   a. Notify and obtain Company's advance written permission before proceeding; and
   b. Ensure that it has a legally approved mechanism in place to allow for the international data transfer, or that Contractors have entered into the Standard Contractual Clauses with Partner set forth in the Attachments.

b. The Company does not sell, license, lease or otherwise disclose Affiliate's personal information to third parties, except as described in this Privacy and Data Protection Policy.

The Company reserves the right to disclose personal information to third parties where such disclosure is required by the Law and/or a regulatory or any other government authority. The Company may also disclose information as necessary to credit reporting or collection agencies as reasonably required in order to provide the services to its clients.

In addition, the Company may engage third parties to help carry out certain internal functions such as account processing, fulfillment, client service, client satisfaction surveys or other data collection activities relevant to its business. Use of the shared information is strictly limited to the performance of the above and is not permitted for any other purpose. All third parties with which the Company shares personal information are required to protect such personal information in accordance with provisions of the GDPR and the Data Processing Legislation and in a manner similar to the way the Company protects the same. The Company will not share personal information with third parties which it considers will not provide its Affiliate's/Partner's the required level of protection.

As part of using your personal information for the purposes set out above, non-affiliated third parties are:

i. service providers and specialist advisers who have been contracted to provide us with services such as administrative, IT, analytics and online marketing optimization, financial, regulatory, compliance, insurance, research and/or other services,
ii. Banks and credit institutions for the processing of payments or bank account operational procedures.
iii. auditors or contractors or other auditing advisors assisting with or advising on any of our business purposes

6. SECURITY STANDARDS

a. Partner shall implement and maintain commercially reasonable and appropriate physical, technical and organizational security measures to protect Personal Data against accidental or unlawful destruction; accidental loss, alteration, unauthorized disclosure or access to personal data transmitted, stored or otherwise processed; all other unlawful forms of Processing; including (as appropriate): (i) the pseudonymisation and encryption of personal data; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and (iv) a process for regularly testing, assessing

and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

b. To the extent that Partner Processes Special Categories of Data, the security measures referred to in this Policy shall also include, at a minimum (i) routine risk assessments of Partner's information security program, (ii) regular testing and monitoring to measure and confirm the effectiveness of the information security program's key controls, systems, and procedures, and (iii) encryption of Special Categories of Data while "at rest" and during transmission (whether sent by e-mail, fax, or otherwise), and storage (including when stored on mobile devices, such as a portable computer, flash drive, PDA, or cellular telephone).

7. USE OF COOKIES

The Company uses cookies to secure clients' activities and to enhance the performance of the http://www.fxvcpartners.com website. Cookies used by the Company do not contain personal information or other sensitive information. The cookies used by the company are:

- "persistent cookies"- only read by our website, are stored on your devise for a fixed time period and are not deleted when the browser is closed. We use these cookies to know who you are for your next visits allowing us to know your preferences the next time you log-in.
- "session cookies"- these are only stored while the browsing session lasts enabling the normal use of the system and are deleted when the browser is closed.

Please note that you may remove the cookies following your browser settings however, disabling of cookies may limit your online experience as well as the functionality of some of the features for the services we provide may be low.

The Company may share website usage statistics with Affiliates/Partners. It is noted that the information collected by Affiliate / Partners is not personally identifiable. To administer and improve the http://www.fxvcpartners.com website, the Company may use third parties to track and analyze usage and statistical volume information. The third party may use cookies to track behaviour and may set cookies on behalf of the Company. These cookies do not contain any personally identifiable information.

8. GENERAL

a. If any of the Data Protection Laws are superseded by new or modified Data Protection Laws (including any decisions or interpretations by a relevant court or governmental authority relating thereto), the new or modified Data Protection Laws shall be deemed to be incorporated into this Policy, and Partner will promptly begin complying with such Data Protection Laws.

b. The Company reserves the right to update it Privacy Policy from time to time. In them even the Company materially changes this Policy including how it collects, processes or uses Affiliates / Partners personal information, the revised Policy will be uploaded on the Company's website accordingly. In this respect, the Affiliates / Partners hereby agree to accept posting revised Policy electronically on the website as the actual notice of the Company to the Affiliates / Partners. Any dispute over the Company's Privacy Policy is subject to this notice and the Affiliates Agreement.

The Company encourages its Affiliates / Partners to periodically review this Policy so that they are always aware of what information the Company collects, how it is processed and used and to whom it may be disclosed in accordance with the provisions of this Policy.

c. Any ambiguity in this Policy shall be resolved to permit Company to comply with all Data Protection Laws. In the event and to the extent that the Data Protection Laws impose stricter obligations on the Partner than under this Policy, the Data Protection Laws shall prevail.

d. If this Policy does not specifically address a particular data security or privacy standard or obligation, Partner will use appropriate, generally accepted practices to protect the confidentiality, security, privacy, integrity, availability, and accuracy of Personal Data.

e. Partner agrees that, in the event of a breach of this Policy, neither Company nor any relevant Company's customer will have an adequate remedy in damages and therefore either Company or an affected customer shall be entitled to seek injunctive or equitable relief to immediately cease or prevent the use or disclosure of Personal Data not contemplated by the Agreement and to enforce the terms of this Policy or ensure compliance with all Data Protection Laws.

f. If Partner is unable to provide the level of protection as required herein, Partner shall immediately notify Company and cease processing. Any non-compliance with the requirements herein shall be deemed a material breach of the Agreement and Company shall have the right to terminate the Agreement immediately without penalty.

g. Company, shall have the right to: (a) require from Partner all information necessary to, and (b) conduct its own audit and/or inspections of Partner (including its facilities or equipment involved in the Processing of Personal Data) in order to: demonstrate compliance with the Policy and the applicable Attachments. Such audit and/or inspection shall be conducted with reasonable advanced notice to Partner, and shall take place during normal business hours to reasonably limit any disruption to Partner's business.

h. On termination of the Policy and at the option of the Company, the Partner shall promptly return or delete Personal Data and certify in writing that it has done so. The Partner may retain a copy of Personal Data only if it is obliged to do so by EU Law. "**EU Law**" means European Union law, the law of any state that is a Member State of the European Union on the date of this Policy and the law of any state that subsequently becomes a Member State of the European Union.

i. The obligations in this Policy shall apply in addition to any existing contractual terms between the Company and the Partner and shall not replace or reduce any obligations of the Partner as these might exist.

j. This Policy is intended to benefit the Company and Partner and any third party who is granted contractual third-party rights under the contractual arrangement between the Company and the Partner. Otherwise this Policy does not create any contractual third-party rights.

k. This Policy shall be governed by the laws of the Republic of Cyprus and any dispute shall be settled exclusively by the laws and Courts of the Republic of Cyprus.

IN WITNESS WHEREOF this Policy has been signed by the Partner:

Partner

By: _____

Title: _____

Date: _____

Signature: _____

EXHIBIT A – STANDARD CONTRACTUAL CLAUSES (PROCESSOR)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

For purposes of this Exhibit A:

any reference to "data exporter" means Company, acting as data exporter, and
any reference to "data importer" means Partner or Partner's Contractor

each a "**Party**"; together the "**Parties**".

The Parties have agreed on the following Standard Contractual Clauses (the "**Clauses**") in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the

event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely the Republic of Cyprus.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely the Republic of Cyprus

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

Clause 13

Indemnification

The parties agree that if data exporter is held liable for a violation of the clauses committed by the data importer, the data importer will, to the extent to which it is liable, indemnify the data exporter for any cost, charge, damages, expenses or loss it has incurred.

APPENDIX 1 TO EXHIBIT A

This Appendix 1 forms part of the Clauses and must be completed and signed by the parties. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is the Company. Activities relevant to the transfer include the performance of services for Company and customers.

Data importer

The data importer is the Partner. Activities relevant to the transfer include the performance of services for Company under the Agreement.

Data subjects

The personal data transferred may concern the following categories of data subjects:

- Company's end users;

- Company's employees;

- Affiliates and partners.

Categories of data

The personal data transferred may concern the following categories of data:

- Profile data (name, age, gender, physical address, telephone number, email address);

- Financial and payment data (e.g. credit card number, transactions and past transactions);

- Governmental IDs (passport copy or driver's license);

- Other: [complete].

Processing operations

The personal data transferred may be subject to the following basic processing activities, as may be further set forth in contractual agreements entered into from time to time between the Company and customers:

- Customer service activities, such as processing orders, providing technical support and improving offerings;

- Sales and marketing activities;

- Consulting, professional, security, storage, hosting and other related services;

-Internal business processes and management, fraud detection and prevention, and compliance with governmental, legislative and regulatory bodies].

	Data Importer	**Data Exporter**
By:	_____	_____
Title:	_____	_____
Date:	_____	_____
Signature:	_____	_____

APPENDIX 2 TO EXHIBIT A
TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(c), 4(d) and 5(c).

1. Security Management

Partner maintains a written information security management system (ISMS), in accordance with this Appendix, that includes policies, processes, enforcement and controls governing all storage/processing/transmitting of Personal Data, designed to (a) secure Personal Data against accidental or unlawful loss, access or disclosure; (b) identify reasonable foreseeable and internal risks to security and authorized access to Partner Network, and (c) minimize security risks, including through risk assessment and regular testing. The information security program will include the following measures:

Partner actively follows information security trends and developments as well as legal developments with regards to the services provided and especially with regards to Personal Data and uses such insights to maintain its ISMS, as appropriate.

To the extent Partner process cardholder or payment data (such as payment or credit cards), Partner will maintain its ISMS in accordance with the PCI DSS standard, augmented to cover Personal Data, or such other alternative standards that are substantially equivalent to PCI DSS for the establishment, implementation, and control of its ISMS. Additionally, Partner will be assessed against PCI DSS annually by an on-site assessment carried out by an independent QSA (Qualified Security Assessor) and upon Company's request, not to exceed once annually, Partner will provide customer with PCI DSS Attestation of Compliance.

2. Maintain an Information Security Policy

Partner's ISMS is based on its security policies that are regularly reviewed (at least yearly) and maintained and disseminated to all relevant parties, including all personnel. Security policies and derived procedures clearly define information security responsibilities including responsibilities for:

- Maintaining security policies and procedures,
- Secure development, operation and maintenance of software and systems,
- Security alert handling,
- Security incident response and escalation procedures,
- User account administration,
- Monitoring and control of all systems as well as access to Personal Data.

Personnel is screened prior to hire and trained (and tested) through a formal security awareness program upon hire and annually. For service providers with whom Personal Data is shared or that could affect the security of Personal Data a process has been set up that includes initial due diligence prior to engagement and regular (typically yearly) monitoring.

Personal Data has implemented a risk-assessment process that is based on ISO 27005.

3. Secure Networks and Systems

Partner has installed and maintains a firewall configuration to protect Personal Data that controls all traffic allowed between Partner's (internal) network and untrusted (external) networks, as well as traffic into and out of more sensitive areas within its internal network. This includes current documentation, change control and regular reviews.

Partner does not use vendor-supplied defaults for system passwords and other security parameters on any systems and has developed configuration standards for all system components consistent with industry-accepted system hardening standards.

4. Protection of Personal Data

Partner keeps Personal Data storage to a minimum and implements data retention and disposal policies to limit data storage to that which is necessary, in accordance with the needs of its customers. The Personal Date will be kept by the Company during our contractual relationship and 7 (seven) years following the termination of the contractual relationship.

Partner uses strong encryption and hashing for Personal Data anywhere it is stored. Partner has documented and implemented all necessary procedures to protect (cryptographic) keys used to secure stored Personal Data against disclosure and misuse. All transmission of Personal Data across open, public networks is encrypted using strong cryptography and security protocols.

5. Vulnerability Management Program

Partner protects all systems against malware and regularly updates anti-virus software or programs to protect against malware – including viruses, worms, and Trojans. Anti-virus software is used on all systems commonly affected by malware to protect such systems from current and evolving malicious software threats.

Partner develops and maintains secure systems and applications by:

- Having established and evolving a process to identify and fix (e.g. through patching) security vulnerabilities, that ensures that all systems components and software are protected from known vulnerabilities,
- Developing internal and external software applications, including web-applications, securely using a secure software development process based on best practices, e.g. such as code reviews and OWASP secure coding practices, that incorporates information security throughout the software-development lifecycle,
- Implementing a stringent change management process and procedures for all changes to system components that include strict separation of development and test environments from production environments and prevents the use of production data for testing or development.

6. Implementation of Strong Access Control Measures

"**Partner Network**" means the Partner's data center facilities, servers, networking equipment, and host software systems (e.g. virtual firewalls) as employed by the Partner to process or store Personal Data.

The Partner Network will be accessible to employees, contractors and any other person as necessary to provide the services to the Company. Partner will maintain access controls and policies to manage what access is allowed to the Partner Network from each network connection and user, including the use of

firewalls or functionally equivalent technology and authentication controls. Partner will maintain corrective action and incident response plans to respond to potential security threats.

Partner strictly restricts access to Personal Data by business need to know to ensure that critical data can only be accessed by authorized personnel. This is achieved by:

- Limiting access to system components and Personal Data to only those individuals whose job requires such access and
- Establishing and maintaining an access control system for systems components that restricts access based on a user's need to know, with a default "deny-all" setting.

Partner identifies and authenticates access to all systems components by assigning a unique identification to each person with access. This ensures that each individual is uniquely accountable for their actions and any actions taken on critical data and systems can be traced to known and authorized users and processes. Necessary processes to ensure proper user identification management, including control of addition/deletion/modification/revocation/disabling of IDs and/or credentials as well as lock out of users after repeated failed access attempts and timely termination of idling session, have been implemented.

User authentication utilizes at least passwords that have to meet complexity rules, which need to be changed on a regular basis and which are cryptographically secured during transmission and storage on all system components. All individual non-console and administrative access and all remote access use multi-factor authentication.

Authentication policies and procedures are communicated to all users and group, shared or generic IDs/passwords are strictly prohibited.

7. Restriction of Physical Access to Personal Data

Any physical access to data or systems that house Personal Data are appropriately restricted using appropriate entry controls and procedures to distinguish between onsite personnel and visitors. Access to sensitive areas is controlled and includes processes for authorization based on job function and access revocation for personnel and visitors.

Media and backups are secured and (internal and external) distribution is strictly controlled. Media containing Personal Data no longer needed for business or legal reasons is rendered unrecoverable or physically destroyed.

8. Regular Monitoring and Testing of Networks

All access to network resources and Personal Data is tracked and monitored using centralized logging mechanisms that allow thorough tracking, alerting, and analysis on a regular basis (at least daily) as well as when something does go wrong. All systems are provided with correct and consistent time and audit trails are secured and protected, including file-integrity monitoring to prevent change of existing log data and/or generate alerts in case. Audit trails for critical systems are kept for a year.

Security of systems and processes is regularly tested, at least yearly. This is to ensure that security controls for system components, processes and custom software continue to reflect a changing environment. Security testing includes:

- Processes to test rogue wireless access points,

- Internal and external network vulnerability tests that are carried out at least quarterly. An external, qualified party carries out the external network vulnerability tests.
- External and internal penetration tests using Partner's penetration test methodology that is based on industry-accepted penetration testing approaches that cover the all relevant systems and include application-layer as well as network-layer tests

All test results are kept on record and any findings are remediated in a timely manner.

Partner does not allow penetration tests carried out by or on behalf of its customers.

In daily operations IDS (intrusion detection system) is used to detect and alert on intrusions into the network and file-integrity monitoring has been deployed to alert personnel to unauthorized modification of critical systems.

9. Incident Management

Partner has implemented and maintains an incident response plan and is prepared to respond immediately to a system breach. Incident management includes:

- Definition of roles, responsibilities, and communication and contact strategies in the event of a compromise, including notification of customers,
- Specific incident response procedures,
- Analysis of legal requirements for reporting compromises,
- Coverage of all critical system components,
- Regular review and testing of the plan,
- Incident management personnel that is available 24/7,
- Training of staff,
- Inclusion of alerts from all security monitoring systems,
- Modification and evolution of the plan according to lessons learned and to incorporate industry developments.

Partner has also implemented a business continuity process (BCP) and a disaster recovery process (DRP) that is maintained and regularly tested. Data backup processes have been implemented and are tested regularly.

10. Physical Security.

Physical Access Controls. Physical components of the Partner Network are housed in nondescript facilities ("Facilities"). Physical barrier controls are used to prevent unauthorized entrance to Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., contract or in-house security guard service, receptionist, etc.). Employees and contractors are assigned are assigned photo-ID badges that must be worn while the employees and contractors are at any of the Facilities. Visitors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor is at any of the Facilities, and are continually escorted by authorized employees or contractors while visiting the Facilities.

Limited Employee and Contractor Access. Partner provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges

are promptly revoked, even if the employee or contractor continues to be an employee of Partner of its affiliates.

Physical Security Protections. All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. Partner also maintains electronic intrusion detection systems designed to detect unauthorized access to the Facilities, including monitoring points of vulnerability (e.g., primary entry doors, emergency egress doors, etc.) with door contacts, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors is logged and routinely audited.

11. Continued Evaluation

Partner will conduct periodic reviews of the Security of its Partner Network and adequacy of its information security program as measured against industry security standards and its policies and procedures. Partner will continually evaluate the security of its Partner Network to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.