Data Processing Agreement

between

The Client
Hereinafter: the Controller

Sterling Technology Ltd
Hereinafter: the Processor

Collectively hereinafter to be referred to as **"Party"** / **"Parties"**

WHEREAS:

A. Controller and Processor have entered into a Service Agreement, by which Processor provides Virtual Data Room services;

B. The Parties wish to reflect the Parties' agreement regarding the processing of personal data in compliance with the relevant data protection laws and regulations and more specific in compliance with Art. 28 of the EU General Data Protection Regulation;

C. Regarding the processing of personal data the provisions of this Controller-to-Processor Agreement supersedes all previous understandings and agreements between the Parties. In the event of any conflict between the provisions of the Service Agreement and this Controller-to-Processor Agreement the latter shall prevail.

IT IS AGREED AS FOLLOWS:

DEFINITIONS AND INTERPRETATION

"Agreement" this agreement including the attached Annexes;

"Ancillary services" means services which are independent from the subject matter of this Agreement such as telecommunication services, postal / transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment;

"Annex" means each annex to this Agreement which forms part of the agreement;

"Another processor" means any data processor engaged by Processor in the course of providing the Services.

"Controller" means 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;

"Data Protection Laws" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

"EEA" means European Economic Area and consist of all countries of the European Union, Liechtenstein, Norway and Iceland;

"GDPR" means the 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 (General Data Protection Regulation).References to GDPR should be read to include the corresponding requirements in the UK Data Protection Act 2018 (UK GDPR);

"Personal Data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

"Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring,

storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

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

"Services" means all services Processor provides, as agreed to by the Service Agreement;

"Service Agreement" means the agreement the Parties have entered into regarding the provision of services by the Processor, referred to in 'A' above.

1. Object / Scope of the processing

The object / scope of the data processing to be provided by the Processor is stipulated in the Service Agreement which is hereby fully referenced.

2. Duration

This agreement shall run until formally terminated by either the data controller or data processor.

3. Specification of Processing

(1) Nature and purpose of the intended processing

Nature and purpose of processing of personal data on behalf of the Controller are defined in the Service Agreement.

(2) The performance of the contractually agreed processing of data shall be carried out exclusively within the EU / EEA or UK. Each and every transfer of personal data beyond the EU / EEA or UK requires the prior (written or email) approval of the Controller and shall only take place if the specific conditions as laid down in Art. 44 et seq. GDPR have been fulfilled. Following Brexit, and until the UK achieves Adequacy Status, Data processed on behalf of EU / EEA Data

Controllers shall be subject to the Model Clause Annex at the end of this agreement.
Types of Data

The types of personal data processed is defined in the Service Agreement under sec. 10.4

4. Technical and Organizational Measures

(1) Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor is obliged to implement appropriate technical and organizational measures in such a manner that the processing of personal data will meet the requirements of applicable data protection law, in particular the GDPR and this Agreement. The Processor hereby acknowledges and ensures the rights of the affected data subjects as specified above. To this end and in accordance with Art. 32 GDPR Processor shall appropriately document the specific measures and provide it to the Controller for approval. Once mutually agreed on, the technical and organizational measures shall become an integral part of the agreement.

(2) The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. The state of the art, implementation costs, the nature, scope and purposes of processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons within the meaning of Art 32 Paragraph 1 GDPR shall be taken into account.

(3) The technical and organizational measures are subject to technical progress and continuous development. In this context, the Processor is permitted to implement adequate alternative measures. However, the security level of the specified measures may not fall below the herein agreed level. In any case, the technical and organizational measures must correspond to requirements of Sterling Information Security Policies.

(4) Notwithstanding the foregoing, the Processor shall implement a process for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures to ensure the security of the processing as agreed herein. Upon request the Processor shall provide appropriate documentation.

5. Rectification, restriction and erasure of data

(1) The Processor may only rectify, erase or block personal data upon instruction issued by the Controller. In case of requests regarding the rectification or the erasure directly addressed to the Processor by a data subject, the Processor shall forward this request immediately to the Controller.

(2) As far as possible, the Processor shall assist and support the Controller for fulfillment of the Controller´s obligation to respond to requests for exercising the data subject´s right, namely the 'right to be forgotten', rectification, data portability, objections to processing, restriction of processing and access rights.

6. Processor´s obligations

In addition, to be compliant with the rules and obligations laid down herein, the Processor shall adhere to the statutory requirements according to Art. 28 - 33 GDPR. This said, the Processor acknowledges in particular the following obligations:

(1) To process the personal data only on documented instructions from the Controller unless processing is required by applicable laws to which the Processor is subject, in which case the Processor shall, to the extent permitted by applicable laws, inform the Controller of that legal requirement before the relevant processing of that personal data. The Processor shall immediately confirm oral instructions in writing or via email.

(2) To inform the Controller immediately if he considers that an instruction violates data protection laws or regulations. The Processor shall then be entitled to suspend the execution of the relevant instructions until the Controller confirms or changes them.

(3) To appoint a data protection officer or, in cases of not being obliged to appoint a data protection officer, another contact person who is responsible for data protection issues. The contact information of the data protection officer or another person responsible shall be given to the Controller for the purpose of establishing direct contact. The Controller shall be informed immediately of any changes thereto.

(4) To maintain a record of processing activities.

(5) To allow access to the personal data only where and to the extent that such access is required and necessary for the performance of the services and subject to such staff and consultants having entered into an adequate non-disclosure agreement and committed themselves to confidentiality.

The Processor and any person acting under the authority of the Processor and / or Controller, who has access to personal data, shall not process those data except on instructions from the Controller, unless required to do so by law.

(6) As far as the subject matter of this Agreement is affected and as far as legally permitted, the Processor shall immediately inform the Controller of any inspections, investigations and / or administrative measures conducted by a supervisory authority.

(7) In cases where the Controller becomes subject to an inspection by the supervisory authority, an administrative offence or criminal procedure, a liability claim by a data subject or by a third party or any other claim related to this Agreement and the data processing by the Processor, the Processor shall make every effort to support the Controller.

(8) The Processor shall inform the Controller as soon as possible about any complaints, requests or other communications received from data subjects, data protection authorities or third parties related to the processing of personal data by the Processor and / or the Controller. Where, in accordance with applicable data protection laws, Controller is obliged to answer a data subject's enquiry related to the processing of such data subject's data, Processor shall support Controller in providing the required information. However, Processor shall not directly respond to any enquiries of data subjects and shall refer such data subjects to the Controller.

7. Subcontracting

(1) The Processor shall not engage another processor (i. e. sub-processor) without the prior specific written authorization by the Controller. Established sub-processors necessary for the provision of contracted services relating to this agreement, are documented within this agreement.

(2) In cases where the Processor engages another processor for carrying out specific processing activities on behalf of the Controller, the same obligations as set out in this Agreement shall be imposed on that other processor by way of a written contract before processing of data by that other processor.

(3) Based on the stipulations in this section

Engaging another processor is not permitted.

(4) The Processor shall provide the Controller in due time with prior notice (written or email) of any new other processor (including full details of the processing to be undertaken by the new processor) or of any changes to the list of other processors in place.

(5) Before another processor first processes Controller´s personal data, the Processor shall carry out adequate due diligence to ensure that the other processor is capable of providing the level of protection for Controller´s personal data required by this Agreement, the Service Agreement and applicable law.

(6) If the Controller has a reasonable basis to object to Processor´s use of another processor, the Controller shall notify the Processor promptly in writing within 30 business days after receipt of data Processor´s notice. For the avoidance of doubt, the Parties agree that unless the Controller can show evidence that the new processor provides an unacceptable risk to the protection of Personal Data (e.g., the other processor has a history of security breaches) or is a competitor of the Controller, it would be unreasonable for the Controller to object if the other processor has passed Processor´s vendor security evaluation.

(7) Notwithstanding the foregoing, if the Controller objects to the engagement of another processor, the Parties will come together in good faith to discuss an appropriate solution. The Processor may in particular choose to: (i) not use the intended processor or (ii) take the corrective steps and / or measures requested by the Controller and engage the processor. If none of these or any other options are reasonably possible and the Controller maintains to object for a legitimate reason, the Controller may terminate the Agreement on 30 days´ written notice.

(8) If and as far as outsourced ancillary services are affected, the Processor shall be obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure adequate data protection and security measures with regard to Controller's data.

8. Audit rights

(1) Upon reasonable advance notice by Controller and in order to ensure and review compliance with the technical and organizational security measures and the obligations laid down in this Agreement, the Processor shall permit the Controller to conduct periodic audits or to have them carried out by an auditor mandated by the Controller. This also includes on-site inspections. The Processor shall, at Controller´s

written request and within a reasonable period of time, submit to Controller any and all information, documentation and other means of factual proof necessary for the audit. The audit result shall be documented appropriately.

(2) In addition, evidence of being compliant may be provided by

(a) Compliance with approved Codes of Conduct and / or

(b) Certification according to an approved certification procedure in accordance with Art. 42 GDPR and / or

(c) Current auditor's certificates, reports or excerpts from reports provided by independent bodies. At the Controller´s request, the Processor will provide Controller with a copy of the audit report signed by the third-party auditor so that the Controller can reasonably verify Processor´s compliance with the technical and organizational measures and obligations under this Agreement.

(3) In cases where the Controller conducts an on-site audit, the Processor will reasonably support the Controller in its audit processes.

9. Data center´s location

(1) The Processor´s data center(s) are located in the UK and in the EU.

(2) The Processor shall not migrate the Controller´s instance to a data center outside the aforementioned and agreed countries without Controller´s prior consent (in writing or via email). If the Processor intends to migrate the Controller´s instance to a data center within the aforementioned and agreed countries, the Processor will notify the Controller in writing or via email.

10. Assisting Obligations

(1) The Processor shall assist the Controller in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations, referred to in Art. 33 to 36 of the GDPR. This includes in particular:

(a) The obligation to report a personal data breach immediately to the Controller;

(b) The duty to assist the Controller with regard to the Controller's obligation to provide information to the data subject concerned and to provide immediately the Controller with all relevant information in this regard. Such information shall as a minimum describe the nature of the data breach, the categories and numbers of data subjects concerned, the categories and numbers of personal data records concerned and the likely consequences of the data breach.

(c) Supporting the Controller with its data protection impact assessment;

(d) Supporting the Controller with regard to the record of processing;

(e) Supporting the Controller with regard to consultation of the supervisory authority.

11. Deletion and return of personal data

(1) After conclusion of the contracted work, or earlier upon request by the Controller, at the latest upon termination of the Service Agreement, the Processor shall hand over to the Controller or – subject to prior consent – destroy all documents, processing and

utilization results, and data sets related to the Agreement that have come into its possession, in a data protection compliant manner. The same applies to any and all connected test, waste, redundant and discarded material. The log of the destruction or deletion shall be provided on request.

(2) Documentation which serves as a proof of proper data processing must be kept by the Processor in accordance with the respective storage terms. The Processor can hand it over to the Controller at the end of the service to be relieved of Processor´s obligations.

12. Liability

(1) The statutory provisions, in particular Art. 82f. GDPR, apply in the event of compensation or liability claims.

(2) Statutory provisions, in particular arising from civil or criminal law, shall apply for miscellaneous liability and (damage) claims.

(3) The contractual penalty set forth herein shall not have any influence on other claims of the Controller.

13. Miscellaneous

(1) This Agreement may be altered or supplemented only in writing and provided any such amendment is signed by the duly authorized representatives of both Parties.

(2) Where Controller´s data becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while in Processor´s control, Processor shall notify Controller of such action without undue delay. Processor shall, without undue delay, notify to all involved parties in such action, that any data affected thereby is in Controller´s sole property and area of responsibility, that data is at Controller´s sole disposition, and that Controller is the responsible body in terms of applicable data protection laws.

(3) If any provision of this Agreement is held invalid, illegal, or unenforceable for any reason, such provision shall be severed and the remainder of the provisions hereof shall continue in full force and effect as if this Agreement has been executed with the invalid provision eliminated.

(4) This Agreement is governed by the laws of England & Wales.

If the data controller is based in the EEA (post Brexit), then the model clauses in schedule A shall apply.

SCHEDULE A

PERSONAL DATA PROCESSING PURPOSES AND DETAILS

Subject matter of processing:

Business Information stored for reference as part of business due diligence activities

Duration of Processing:

As per contracted periods defined In service level agreements

Nature of Processing:

Storage of Information In SaaS hosted environment

Potential viewing of personal data as part of technical support activities

Business Purposes:

Provision of contracted services

Personal Data Categories:

Personal data associated with entities as part of the due diligence process, may Include special category data depending upon the business activities being performed by the business.

Data Subject Types:

Employees, B2B Clients, B2C Clients and Suppliers

Authorised Persons:

Staff Involved with customer and technical support

Processor's legal basis for processing Personal Data outside the EEA in order to comply with cross-border transfer restrictions:

- Lawful grounds based on Contractual necessity and all processing Is carried out In line with contractual requirements.
- Standard Contractual Clauses between Processor as "data exporter" on behalf of Controller and Processor affiliate or subcontractor as "data importer".
  Approved Subcontractors:

Amazon Web Services, (Hosting Service Provider), has no access to any data stored In the hosted environment

SCHEDULE B

STANDARD CONTRACTUAL CLAUSES

Standard Contractual Clauses for the transfer of personal data from the European Union to processors established in third countries (controller to processor transfers)

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

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, these contractual clauses shall form part of the contractual agreement between the client (the data exporter),

And

Sterling Technology Limited (the data importer)
Address: First Floor, 5 Fleet Place, London, United Kingdom, EC4M 7RDTel: +44 20 7100 9680
E-mail: dpo@sterlingvdr.com

Other information needed to identify the organisation:

Registered Office: 11124057

each a 'party'; together 'the parties',

HAVE AGREED on the following 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 Schedule 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 (1);

(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 Schedule 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 Schedule 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 Schedule 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 (2)

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 Schedule 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 Schedule 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 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 …

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 (3). 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…

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.

On behalf of the data importer:

Name (written out in full) and position: Geoff Keating, CEO
Address: 33 Aldgate House, Aldgate High Street, London,
England, EC3N 1AH

Signature: Geoff Keating

Schedule 1

to the Standard Contractual Clauses

This Schedule 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 Schedule

Data exporter

The data exporter is:

Accessing and storing company information in securely hosted storage environments supported by technical and customer service staff based outside of the EU.

Data importer

The data importer is:

Securely hosted storage environments supported by technical and customer service staff based outside of the EU.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Personal Data associated with organisational due diligence activities, including staff, customers and suppliers

Categories of data

The personal data transferred concern the following categories of data (please specify):

All categories of data may be stored or accessed within the platform related to the activities of the organisations to which the due diligence applies

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

All categories of special category data related to the activities of the organisations to which the due diligence applies

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

Storage and viewing of information in the fulfilment of contracted service provision, including technical support and customer service.

Schedule 2

to the Standard Contractual Clauses

This Schedule forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

1. Technical and operational security measure have been adopted in line with the requirements of ISO27001, to which the Data Importer is certified by a UKAS accredited certification body.

2. The associated controls are all documented as part of a Statement of Applicability which covers the full scope of personal data processed by the Data Importer.