Data Processing Addendum 1

This Addendum on Data Processing (hereinafter: "Addendum") is made on the Effective Date, by and between:

Customer as defined by the SOW

– hereinafter referred to as "**Controller**" –

and

Datasite entity as defined by the SOW

– hereinafter referred to as "**Processor**" –

Hereinafter each individually referred to also as the "**Party**" and collectively as the "**Parties**"

Preamble:

(A) The Parties have entered into an Agreement which outlines the Services to be provided (definitions provided in Section 1 below). As part of the provision of Services by the Processor, Personal Data may be transferred by the Controller to the Processor.

(B) In the event of any conflict between the provisions in this Addendum and the provisions set forth in the Agreement, the provision or provisions of this Addendum will prevail. Capitalized terms not defined in this Addendum are defined in the Agreement.

(C) To ensure compliance by the Parties with Processing obligations pursuant to the Data Protection Rules, as amended from time to time, the Parties hereby agree as follows:

1. Definitions

1.1. "**Appendix**" means the appendix annexed to and forming an integral part of this Addendum;

1.2. "**Data Protection Country**" or "Data Protection Countries" means a country or countries where privacy, data protection or information security laws are in place that regulate personal or private information or Personal Data, including but not limited to the European Economic Area, Brazil, Hong Kong, Australia, Singapore, Canada, United Kingdom and Switzerland.

1.3. "**Data Protection Rules**" means the relevant national laws that apply to the Processing of Personal Data in Data Protection Countries, including but not limited to any applicable privacy and information security laws and regulations that apply from time to time;

1.4. "**Data Subject**" means an identified or identifiable natural person whose Personal Data is subject to Processing; an identifiable person is one who can be identified, directly or indirectly, 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 physical, physiological, genetic, mental, economic, cultural or social identity;

1.5. "**Information Security Incident**" means any transfer, access and disclosure to third parties, or Processing in breach of this Addendum or the Data Protection Rules or any event directly or indirectly affecting the confidentiality, integrity, authenticity of Personal Data;

1.6. "**Privacy Shield**" means the EU-U.S. Privacy Shield Framework, which became effective August 1, 2016, and Swiss-US Privacy Shield Framework, which became effective April 12, 2017.

1.7. "Agreement" means the Statement of Work and the General Terms and Conditions between the Controller and the Processor;

1.8. "**Personal Data**" means any information relating to a Data Subject contain within the Content.

1.9. "**Process**", "**Processing**" or "**Processed**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic 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, blocking, erasure or destruction;

1.10 "**Services**" means the provision of services as described in the Agreement and this Addendum;

1.11 "**Special Categories of Data**" means the Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data that uniquely identify a natural person, as well as Personal Data concerninghealth, sex life or sexual orientation

2. Processing Activities

The Controller shall have sole responsibility for the accuracy, quality, and legality of Processing of Personal Data, and shall comply with and is responsible for its invited Users compliance with applicable Data Protection Rules. The Processor agrees to Process the Personal Data to provide Services in accordance with this Addendum and the Agreement, pursuant to Controller's written instructions as set forth in Appendix 1 of this Addendum, and as may be communicated by the Controller from time to time. If the Processor believes that an instruction infringes applicable Data Protection Rules, it will immediately notify the Controller. The Processor undertakes to Process the Personal Data in accordance with applicable Data Protection Rules.

3. Duration and Termination of this Addendum

3.1. This Addendum is effective as of the Effective Date and shall remain in force during the term of the Agreement. This Addendum will terminate automatically with the termination or expiry of any SOW.

3.2. Notwithstanding the termination of this Addendum, the Processor and any subcontractors shall continue to be bound by their obligations of confidentiality.

4. International Transfers

The Processor is certified under Privacy Shield frameworks and is committed to its principles. Controller acknowledges that Processor may Process Personal Data outside the EEA, United Kingdom and United States; however, Personal Data will continued to be stored in a Data Protection Country or in the United States. The Processor will only onward transfer Personal Data in compliance with Data Protection Rules and notify Controller if it can no longer provide adequate level of protection as required by Data Protection Rules.

5. Confidentiality and Information Security Standards

5.1. The Processor shall keep Personal Data strictly confidential. The Processor shall ensure that its employees are aware of the applicable privacy and information security requirements and are held by legally binding confidentiality obligations.

5.2. The Processor will implement appropriate operational, technical and organizational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, access described in Appendix 2.

5.3. The Processor will update the technical and organizational security measures in line with reasonable technological developments as determined by Processor and provide updated documentation to the Controller on request in the form of its current ISO 27001 certification.

6. Cooperation and Notification Obligations

6.1. The Parties will co-operate with each other to promptly and effectively handle enquiries, complaints, and claims relating to the Processing of Personal Data from any government authority or Data Subjects. If a Data Subject should apply directly to the Processor to exercise his/her Personal Data rights, the Processor must forward this request to the Controller without undue delay. The Processor will notify the Controller immediately if the Personal Data is subject to a control or investigation by public authorities and will not disclose any Personal Data without the prior consent of the Controller. The Processor will provide the public authorities, upon request, with information regarding Processingunder this Addendum as well as allow inspections within the scope stated in this Section 7.

6.2. The Processor will notify the Controller of an Information Security Incident that is determined to affect Controller's Personal Data without undue delay. The Processor shall provide Controller with the information to help and reasonably assist Controller as required by Data Protection Rules.

7. Controller's Audit and Inspection Rights

Upon Controller's request, Processor shall make available to Controller information necessary to demonstrate Controller's compliance with the obligations in the Addendum and Data Protection Rules and allow for and contribute to audits, including inspections conducted by Controller or an independent third party auditor mandated by Controller for the purpose of verifying the Processor's compliance with this Addendum, subject to the persons performing such audit sign a non-disclosure agreement with the Processor. All inspections shall be conducted during normal working hours and

without interfering with the course of the Processor's business.

8. Use of Subcontractors

8.1 Controller hereby acknowledges and agrees that Processor may use Subcontractors to Process Personal Data. Processor will make available to Controller its current list of Subcontractors upon request. Any Subcontractor will be permitted to Process Personal Data only to deliver the Services Processor has retained them to provide and will be contractually bound by contractual obligations no less protective than this Addendum. Processor shall be liable for the acts and omissions of any Subcontractor as if the acts or omissions were performed by Processor. The Processor will keep the Controller updated of any changes to the subcontracted Processing and provide the Controller with a copy of this subcontracting agreement upon request.

8.2 If the Processor intends to appoint or replace a Subcontractor covered by this Addendum, the Processor shall inform Controller of this advance and give Controller the opportunity to reasonably object to such changes. The Supplier shall provide Controller with all information that Controller may reasonably request to assess whether the appointment of the proposed Subcontractor complies with the Controller's obligations under this Addendum and applicable Data Protection Rules.

9. Return and Deletion of Personal Data

Upon the request of the Controller or upon termination of this Addendum, the Processor will, return or destroy all Personal Data and copies thereof. Upon the request of the Controller, the Processor will certify that this has been done.

10. Liability & Indemnification

10.1 The Liability of the Parties and the limitation thereof shall be in accordance with the Agreement.

10.2 The Controller shall indemnify Processor against all claims by any third party with regard to the processing of personal data provided to the Processor if the processing of such data was not permitted by Data Protection Rules.

Controller:	**Processor:**
By:_____	By:_____
Name/Title:_____	Name/Title:_____
Date: _____	Date:_____

Appendix 1: Processed Personal Data and Purposes

Personal Data are transferred and Processed for the **following purposes**:

- Secure online repository and data sharing for corporate due diligence, related transactions or internal business purposes.

Scope of Processing:

- As described in the Statement of Work, Processor provides virtual data room, a secure online repository for storing, managing, collaborating on and distributing data and documents.

Categories of Personal Data:

- Names, address, company email address, company phone number, national identification numbers, compensation and benefits, holiday and pension information, job titles and functions and potentially all other types of personal data embedded in the business information uploaded by Controller's Administrator onto the virtual data room.

Special Categories of Data (if applicable):

The Personal Data concerns the following Special Categories of Data (please specify):

- None, unless otherwise identified by Controller

Data Subjects:

The Personal Data concerns the following categories of Data Subjects:

- Business information that may include owner, employee, customer, contractor and vendor data.

Appendix 2: Information Security Measures

Appendix 2 includes:

Section I: Processor's General Data Security Plan
Section II: Processor's Information Security Procedure/Process

I. General Data Security Plan

The Processor undertakes to institute and maintain the following data protection measures:

	Security Requirement	How the Processor implements the specific information security measure
	Please describe the access control (physical) measures in your company to prevent unauthorized persons from gaining access to Processing systems within which Personal Data are Processed or used (If your company has several subsidiaries or branches please distinguish the differences between the locations).	All data centers hold ISO 27001:2013 and SOC 2 Type 2 certifications. In addition, the data centers are certified under the Privacy Shield Frameworks. A perimeter of multiple security controls are in place for all data centers which include multiple require authentication methods in order to gain access.
2.	Please describe the admission control measures taken in your company to prevent Processing systems from being used without authorization.	Authorized users are based on business requirements and require management role identification and approval. Time out features, strong authentication requirements and access rights are implemented and trackable.
3.	Please describe the access control (virtual) measures taken in your company to ensure that persons entitled to use a Processing system have access only to Personal Data to which they have a right of access, and that Personal Data cannot be read, copied, modified or removed without authorizations in the course of Processing or use and after storage.	Authorized user access is managed through a formal registration and de-registration procedure for granting and revoking access to all systems and services based on job role. Audit reporting allows for the accurate monitoring of user activity and access controls are in place to protect data integrity and confidentiality.
4.	Describe the transmission control measures taken in your company to ensure that Personal Data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of Personal Data by means of data transmission facilities are envisaged.	Processor has removable media policy with the appropriate technical controls in place to protect data integrity and confidentiality and prohibit unauthorized Personal Data transfer. Remote access is controlled using multifactor authentication. Data is encrypted at rest and in-transit using government approved encryption technologies.

5.	Describe the measures of input control to ensure that it is possible to check and establish whether and by whom Personal Data have been entered into Processing systems, modified or removed.	Processor is agnostic to the data the client chooses to upload. All user actions with respect to data integrity and confidentiality are tracked and reportable. Controller has sole determination on what data is provided to Processor.
6.	Describe the assignment control measures in your company to ensure that, in the case of commissioned Processing, the Personal Data are Processed strictly in accordance with the instructions.	Audits are conducted annually as part of ISO 27001 Certification and SOC 2 Type 2 Report to ensure compliance requirements are being met. Authorized users complete Training and acknowledge compliance with company code of conduct and policies annually. All employees and contractors are required to sign NDA.
7.	Describe the availability control measures your company takes to ensure that Personal Data are protected from accidental destruction or loss.	Processor has redundancy with each platform and maintains logs of system availability. In addition, redundancy allows for continuous system backups. Processor has Disaster Recovery and Business Continuity Plans that are reviewed, updated and tested annually.
8.	Describe the separation control measures your company has taken to ensure that Personal Data collected for different purposes can be Processed separately.	Logical separation is maintained within the same multi-tenant database. Authorized users are restricted to the project to which they are authenticated. Processor maintains a 3-tiered application with separation of data; development, test and production.

II. Processor's Information Security Procedure/Process

The Processor implements and follows the following standards, processes, and procedures:

Datasite operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2013 for the following scope: The management of information security applies to processes for the protection of client information regarding the global services of financial transactions and reporting, marketing and communications for regulatory industries, and customer content and collaborations.