DATA PROCESSING ADDENDUM

This Data Processing Addendum ("Addendum") forms part of and supplements the agreement between **Legility, LLC and/or its Affiliate(s)** (collectively, "**Legility**") and the entity you represent ("**Client**") and entered into in connection with Legility's Services which may include the processing of Agreement Personal Data ("**Agreement**"), and is subject to and hereby incorporates by reference the terms and conditions set forth therein.

Client and Legility acknowledge that, as part of the eDiscovery and legal services provided by Legility, Client, as a Controller, may decide to transfer or grant access to Personal Data to Legility as a Processor.

1.   **Definitions and Interpretation**.

1.1   For purposes of this Addendum, the following terms shall mean as follows:

"**Affiliate**" means, with respect to a party, an entity that is Controlled by, Controlling or in common Control with that party, where "**Control**", "**Controlled**", "**Controlling**", and "in common Control with" means the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting shares, by contract or otherwise.

"**Agreement Personal Data**" means any Personal Data (including sensitive or special categories of data) that is processed under or in connection with the Agreement.

"**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 Law(s)**" means applicable data protection laws governing the protection of individuals with regards to the processing of Personal Data including (i) the General Data Protection Regulation (EU) 2016/679 ("GDPR"), (ii), legislation that, replaces or converts into domestic law the GDPR or any other law relating to data protection and privacy as a consequence of the United Kingdom leaving the European Union;; (iv) the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 *et seq.*, and its implementing regulations ("CCPA"); any other similar laws and regulations that prescribe requirements applicable to service providers of Personal Data.

"Data Subject" means a natural person.

"**EU Standard Contractual Clauses**" means the standard contractual clauses for the transfer of Personal Data to processors established in countries outside the European Union which do not ensure an adequate level of protection as set out in Commission Decision C(2010)593 of 5 February 2010, as updated, amended, replaced or superseded from time to time by the European Commission.

"**Personal Data**" means any data that identifies or, alone or in combination with any other data, could reasonably be used to identify, locate, or contact a natural person or household, or any other information that is considered "personally identifiable information," "personal information," "personal data," or other similar terms under applicable Data Protection Law(s).

"**Personal Data Breach**" means any verified breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Agreement Personal Data.

"**Process**", "**Processing**" or "**Processed**" means any operation or set of operations that are performed upon Personal Data, whether or not by automatic means, such as collecting, accessing, processing, using recording, organizing, storing, adapting or altering, retrieving, consulting, disclosing, disseminating, transmitting, aligning or combining, blocking, erasing, destroying or otherwise using in a manner set forth in Data Protection Laws.

"**Processor**" means an entity that processes information only on behalf of the Controller.

"**Sell**" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a Data Subject's Personal Data to a third party for monetary or other valuable consideration.

"**Services**" means performance of the services and activities provided pursuant to or in connection with the Agreement previously entered into between Legility, and in addition to any other services described in the Agreement for which Legility receives or accesses Agreement Personal Data.

"**Service Provider**" means an entity that processes information on behalf of a business and to which the business discloses a Data Subject's Personal Data for a business purpose pursuant to a written contract.

"**Subprocessor**" shall mean a Legility processor engaged by Legility to carry out specific processing activities on Agreement Personal Data.

"**Supervisory Authority**" means any local, national or multinational agency, department, official, parliament, public or statutory person or any other government or professional body, regulatory or supervisory authority, board or other body responsible for administering applicable Data Protection Laws.

2. **Data Protection Obligations**.

2.1 **Role of the Parties**. With respect to the Agreement Personal Data Processed pursuant to the Services Legility provides under the terms of the Agreement or otherwise to Client, Legility acts as a Processor on behalf of Client who is a Controller in respect of the Agreement Personal Data.

2.2 **Compliance with Data Protection Laws**. Each party undertakes to comply with Data Protection Laws applicable to it in its respective role and to the Processing of Agreement Personal Data and will not knowingly cause the other to breach Data Protection Laws. The description of the processing and any specific processing instructions with respect to Personal Data, in addition to those stated in Exhibit B, shall include any relevant descriptions or instructions set forth in the Agreement. In its capacity as a Controller, Client confirms that all Agreement Personal Data collected or sourced by it or on its behalf for Processing in connection with the Services and the performance of the Agreement or which was otherwise made available to Legility shall comply with and have been collected or otherwise obtained in compliance with Data Protection Laws, including ensuring that there is a lawful basis for each Processing activity which Client instructs Legility to perform in relation to the Agreement.

2.3 **Scope of Processing**. Client instructs Legility to Process Agreement Personal Data in accordance with applicable Data Protection Laws: (i) to provide the Services; (ii) as documented in the Agreement (or any statement of work entered into under the Agreement, if applicable), including this Addendum; and (iii) as further documented in any other written instructions given by Client and acknowledged by Legility as constituting instructions for purposes of this Addendum.

3. **Use of Personal Data**. Legility, as a Service Provider, agrees not to Sell Agreement Personal Data. Legility will not retain, use or disclose Agreement Personal Data for any purposes other than specified herein, including, without limitation, performing the Services. If Legility is legally required by Data Protection Laws, or other applicable law, to Process Client Personal Data otherwise than as instructed by Client, Legility will notify Client before such Processing occurs, unless the law requiring such Processing prohibits Legility from notifying Client on an important ground of public interest, in which case Legility will notify Client as soon as that law permits Legility to do so. Legility may aggregate, de-identify, or anonymize Personal Data, so that it no longer meets the Personal Data definition, and may use such aggregated, de-identified, or anonymized data for its own research and development purposes. Legility will not attempt to or actually re-identify any previously aggregated, de-identified, or anonymized data.

4. **Security**. Legility shall implement appropriate technical and organizational security measures to ensure a level of security appropriate to the risks that are presented by the Processing and the nature of the

Agreement Personal Data to be protected, including, as may be appropriate, (i) pseudonymisation and encryption; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of the processing systems and services; (iii) the ability to restore the availability and access to the Agreement Personal Data in a timely manner in the event of a physical or technical incident; and (iv) a process for regulatory testing, assessing and evaluating the effectiveness of those measures. Without prejudice to Legility's data security obligations under this Addendum, Client is responsible for its use of the Services and its storage of Agreement Personal Data outside of Legility's or Legility's Subprocessors' systems, including: using the Services and reasonable additional security controls to ensure a level of security appropriate to the risk in respect of the Agreement Personal Data; securing the account authentication credentials, systems and devices Client uses to access the Services; and retaining copies of its Agreement Personal Data as appropriate.

5.   **Legility Employee Confidentiality**. Legility personnel who have access to Agreement Personal Data are both (i) informed of the confidential nature of the Agreement Personal Data and obliged to keep such Agreement Personal Data confidential; and (ii) aware of Legility's duties and obligations under the Agreement and this Addendum.

6.   **Rights of Data Subjects**.

6.1   **Data Subject Requests.** Legility shall promptly notify Client if it receives a request from a Data Subject to exercise the Data Subject's rights under the applicable Data Protection Law ("Data Subject Request"). Taking into account the nature of the Processing, Legility will use commercially reasonable and appropriate technical and organizational measures to assist Client with the fulfilment of its legal obligation(s) to respond to the Data Subject Request. To the extent legally permitted, Client shall be responsible for any costs arising from Legility's provision of such assistance.

6.2   **Personal Data Breach**. Legility will, upon becoming aware, notify Client without undue delay, of any Personal Data Breach and will provide reasonable assistance to Client in response to such Personal Data Breach to enable Client to meet its obligations under applicable Data Protection Laws as regards the notification to supervisory authorities and/or affected Data Subjects. For these purposes, Legility will provide Client such details as Client reasonably requires (to the extent that those are known to Legility) regarding (i) the nature of the Personal Data Breach, including the categories and approximate number of Data Subjects affected; (ii) any investigations into such Personal Data Breach; (iii) the likely consequences of the Personal Data Breach; and (iv) any measures taken, or that Legility recommends, to address the Personal Data Breach, including to mitigate its possible adverse effects. The parties agree that the details set out under (i) to (iv) above may be provided to Client in phases, as the information becomes known to Legility.

7.   **Deletion or Return of Personal Data**. Legility shall return to Client the Agreement Personal Data and, to the extent permitted by applicable law, delete Agreement Personal Data after termination of the Agreement or the expiration of any confidentiality obligations.

8.   **Subprocessors**. Except with respect to Legility's Subprocessors listed in the attached <u>Exhibit A</u>, which are deemed to be approved by Client as applicable (if used), Legility will not engage a Subprocessor to undertake any material Processing of Agreement Personal Data under the Agreement by and between Client and Legility, other than as previously disclosed to Client, unless the new Subprocessor is subject to a written agreement which imposes substantially equivalent obligations on that Subprocessor as are imposed on Legility by Client. Legility will notify Client of its intent to engage a material Subprocessor and in the event Client objects to such Subprocessor, Client and Legility shall cooperate in good faith to make such adjustments as required to satisfy Client's concerns. If, within five (5) days after notice from Legility, Client has not approved Subprocessor, Client or Legility shall have the right to terminate the applicable portion of the Agreement or the applicable purchase order or statement of work.

9. **Audit**.

9.1 **Compliance.** Legility shall, on written request, make available to Client information that is reasonably necessary to demonstrate compliance with Legility's data protection obligations under this Addendum and permit and contribute to audits, including inspections, conducted by Client or auditor mandated by Client, but in case only: (i) if such information and audits are in relation to the Agreement Personal Data processed pursuant to the Agreement; and (ii) to the extent that such information and audits are required under applicable Data Protection Law.

9.2 **Inspection.** Client agrees that any audit or inspection requested in accordance with Section 9.1 above shall be conducted upon not less than fifteen (15) days' prior written notice, not more than once per calendar year, during normal business hours, causing minimal disruption and subject to Legility's obligations of confidentiality. Legility may charge a fee (based on Legility's reasonable costs) for any audit or inspection performed under this Addendum. Legility will provide Client with further details of any applicable fee, and the basis of its calculation, in advance of any such audit or inspection. Client will be responsible for any fees charged by any auditor or inspector appointed by Client to execute any such audit or inspection. Legility may object in writing to an auditor or inspector appointed by Client to conduct any audit or inspection under this Addendum if the auditor or inspector is, in Legility's reasonable opinion, not suitably qualified or independent, a competitor of Legility, or otherwise manifestly unsuitable. Any such objection by Legility will require Client to appoint another auditor or inspector or conduct the audit itself.

10. **Other Provisions**. Client's remedies (including those of any and all affiliates and related entities making any valid claim against Legility) with respect to any breach by Legility of the terms of this Addendum are subject to all applicable restrictions and limitations of liability under the Agreement (which shall be applied as overall restrictions and limitations on the aggregate of all such claims). All provisions of the Agreement shall remain in effect as supplemented by this Addendum. If there is any conflict or inconsistency between this Addendum and the other terms of the Agreement, this Addendum will govern to the extent required by law; otherwise, the terms of the Agreement shall govern in the case of such conflict or inconsistency. This Addendum (which includes the attachments hereto), sets forth the entire agreement between the parties with respect to the matters set forth herein. This Addendum shall not be binding unless and until fully signed and delivered by both parties. The parties may sign and deliver this DPA as pdfs via email or DocuSignThe terms and conditions stated in this Addendum, whether or not related to, or adopted independently of, an existing agreement between Client and Legility. Nothing in this Addendum or the Agreement relieves Client of its own direct responsibilities and liabilities under the Data Protection Laws. Except as modified below, the terms of the Agreement shall remain in full force and effect.

11. **Governing Law**. This Addendum is governed by the law of the country that governs the Agreement and the parties submit to the jurisdiction of the courts referred to in the Agreement without regard to provisions related to conflicts of law.

12. **European Specific Provisions**.

13.1 **GDPR**. Legility will Process Agreement Personal Data in accordance with the GDPR requirements directly applicable to Legility's provision of its Services.

13.2 **Data Protection Impact Assessment.** Upon Client's request, Legility shall provide Client with reasonable assistance needed to fulfill Client's obligation under the GDPR to carry out a data protection impact assessment related to Client's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Legility. Legility shall provide reasonable assistance to Client in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks to the extent required under the GDPR.

13.3 **Transfer Mechanisms for Data Transfers**. Absent such other form of consent rendering a transfer of Personal Data legally permissible under the GDPR, any transfer by Legility and its Subprocessors of Agreement Personal Data from the European Union to a jurisdiction which the European Commission has

not found to offer an adequate level of protection for Personal Data transferred to it from the European Union shall occur only to the extent (i) the relevant "data exporter" and "data importer" execute the EU Standard Contractual Clauses attached as <u>Exhibit C</u> to this Addendum, or delivered under separate cover, with regard to the processing of Agreement Personal Data or (ii) the relevant "data importer" maintains a lawful mechanism approved by the EU Commission or the applicable Supervisory Authority in the European Union. To the extent any transfer of Agreement Personal Data is conducted in accordance with the foregoing sentence, Client hereby consents to such transfer.

The parties have executed this Addendum to be effective as of the date first stated above.

_____ (Client) Signature: _____ Name: _____ Date: _____	**LEGILITY, LLC** Signature: _____ Name: _____ Date: _____

EXHIBIT A

List of Pre-Approved Subprocessors for Services rendered by Legility and its affiliates (if applicable)

1. Relativity ODA, LLC
2. Everlaw, Inc.
3. OpenText (Catalyst)
4. Box, Inc.
5. Reveal Data Corporation (NexLP and Brainspace)
6. Milyli, Inc. (Blackout)
7. Ipro Tech, LLC
8. Iconic Translations Machines Ltd.
9. iBridge, LLC
10. ALT TAB Consulting USA LLC
11. CXS Hikinex, Inc.

EXHIBIT B

DETAILS OF PROCESSING OF PERSONAL DATA

Subject matter and duration of the processing of Client Personal Data

Legility performs eDiscovery and legal services for law firms and in-house legal departments to assist in their legal matters, such as litigation or regulatory investigations. The subject matter, nature, purpose and duration of the processing of the Agreement Personal Data are set out in the Agreement (likely a Statement of Work) and as may be further stated below or elsewhere in this Addendum.

Data Subjects

The Personal Data transferred to processor is determined and controlled by Client in its sole discretion.

Categories of Data

The Personal Data transferred to or accessed by processor includes all relevant information required to deliver requested Services under the Agreement, is determined and controlled by Client in its sole discretion and may include Client's representatives and end clients who are natural persons, including employees, contractors, and customers, and individuals who may be identified in Client's legal matters such as litigation cases or investigations.

Special Categories of Personal Data (if appropriate)

The Personal Data may include special categories of Personal Data the extent of which is determined by and controlled by Client in its sole discretion.

Processing operations

Personal Data will be Processed for the purpose of and to the extent necessary for the performance of the services requested from Legility under the Agreement only and will be subject to the basic processing activities set out in the Agreement for the performance of services.

EXHIBIT C

STANDARD CONTRACTUAL CLAUSES

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

The entity identified as the "Client" in the DPA (the "**data exporter**")

AND

Legility, LLC, a Tennessee limited liability company having its principal offices located at 216 Centerview Drive, Suite 250, Brentwood, TN 37027 (the **"data importer"**) (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 Appendix 1.

Background

The data exporter has entered into a data processing addendum ("DPA") with the data importer. Pursuant to the terms of the DPA, it is contemplated that services provided by the data importer will involve the transfer of personal data to data importer. Data importer is located in a country not ensuring an adequate level of data protection. To ensure compliance with Directive 95/46/EC and applicable data protection law, the controller agrees to the provision of such services, including the processing of personal data incidental thereto, subject to the data importer's execution of, and compliance with, the terms of these Clauses.

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; [*If these Clauses are governed by a law which extends the protection of data protection laws to corporate persons, the words "except that, if these Clauses govern a transfer of data relating to identified or identifiable corporate (as well as natural) persons, the definition of "personal data" is expanded to include those data" are added.*]

b.   *'the data exporter'* means the controller who transfers the personal data. *'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; [*If these Clauses are not governed by the law of a Member State, the words "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" are deleted.*]

d.   *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor 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 subprocessor 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 subprocessor 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;

c.   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 subprocessor 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 subprocessing 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 subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor 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 subprocessing, 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 subprocessing, it has previously informed the data exporter and obtained its prior written consent;

i. that the processing services by the subprocessor will be carried out in accordance with Clause 11;

j. to send promptly a copy of any subprocessor 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 subprocessor 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 subprocessor 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 subprocessor 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 subprocessor 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 subprocessor agrees that the data subject may issue a claim against the data subprocessor 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 subprocessor 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 subprocessor, 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.

2. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, 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.

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 *Subprocessing*

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 subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor 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 subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor 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 subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing 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.

4. The data exporter shall keep a list of subprocessing 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 subprocessor 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 subprocessor 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 exporter:

_____

Name: _____

Position: _____

Address: _____

Signature: _____

Date: _____

On behalf of the data importer:

Legility, LLC

Name: _____

Position: _____

Address: 216 Centerview Drive, Suite 250, Brentwood, TN 37027

Signature: _____

Date: _____

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses.

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 entity identified as "Client" in the DPA.

Data importer

The data importer is: **Legility, LLC**

Subject matter and duration of the processing of Client Personal Data
Legility performs eDiscovery and legal services for law firms and in-house legal departments to assist in their legal matters, such as litigation or regulatory investigations. The subject matter, nature, purpose and duration of the processing of the Agreement Personal Data are set out in the Agreement (likely a Statement of Work) and as may be further stated below or elsewhere in this Addendum

Data Subjects
The Personal Data transferred to processor is determined and controlled by Client in its sole discretion.

Categories of Data
The Personal Data transferred to or accessed by processor includes all relevant information required to deliver requested Services under the Agreement, is determined and controlled by Client in its sole discretion and may include Client's representatives and end clients who are natural persons, including employees, contractors, and customers, and individuals who may be identified in Client's legal matters such as litigation cases or investigations.

Special Categories of data (if appropriate)
The Personal Data may include special categories of Personal Data the extent of which is determined by and controlled by Client in its sole discretion

Processing operations
Personal data will be processed for the purpose of and to the extent necessary for the performance of the services requested from Legility under the Agreement only and will be subject to the basic processing activities set out in the Agreement for the performance of services.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses.

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

Data importer has implemented appropriate technical and organizational security measures to ensure a level of security appropriate to the risks that are presented by the processing and the nature of the Personal Data to be protected which shall be at least equivalent to those described in the Addendum.