TERMS OF SERVICE

These Terms of Service ("**Agreement**") is a legally binding contract between Klarity Intelligence, Inc., with its principal place of business at 564 Market Street, Suite 316, San Francisco, CA 94104 ("**Klarity**"), and you, the customer ("**Customer**" or "**You**"). This Agreement becomes effective upon Customer's signing of an Order Form (as defined below) that references this Agreement ("**Effective Date**"). The Order Form, along with this Agreement, comprises the full and exclusive understanding between Klarity and Customer regarding the access to and use of the services provided by Klarity to Customer under the Order Form ("**Services**"), and it supersedes all prior and contemporaneous agreements or understandings, whether written or oral. Klarity retains the right to amend this Agreement at any time. Your continued use of the Services after any such changes have been made constitute your acceptance of the revised terms.

1. DEFINITIONS

1.1 "**Affiliate**" means any present or future entity controlled by, or under common control with a party.

1.2 "**Users**" means any persons who are authorized by Customer to use the Services, and who have been supplied user identifications and passwords by Customer (or by Klarity at Customer's request), which may include but are not limited to employees, officers, directors, consultants and auditors of Customer.

2. SERVICES AND SUPPORT

2.1 Subject to the terms of this Agreement and any applicable Order Forms, Klarity will provide Customer the Services in accordance with the Service Level Terms and technical support services (Exhibit A), Data Processing Addendum (Exhibit B), Standard Contractual Clauses (Exhibit C), and Artificial Intelligence Addendum (Exhibit D). Unless otherwise provided in an Order Form, the Services and support services are provided on a non-exclusive basis. Klarity will not provide a physical or installed copy of the Services to Customer.

2.2 Customer may order Services from Klarity by entering into a service order in a mutually agreed upon form ("**Order Form**"). Klarity will provide the Services specified in the Order Form during the term specified therein ("**Subscription Term**"). Upon execution, each Order Form will become effective and incorporate this Agreement.

3. PAYMENT OF FEES

3.1 Customer will pay Klarity the then applicable fees described in the Order Form for the Services in accordance with the terms therein ("**Fees**"). Unless otherwise provided in an Order Form, all Fees are quoted and payable in United States dollars. Klarity reserves the right to change the Fees or applicable charges and to institute new charges and Fees at the end of the Initial Subscription Term, upon sixty (60) days prior notice to Customer (which may be sent by email).

3.2 Unless otherwise stated, the fees described in the Order Form are based on the number of documents purchased in the Order Form ("**Service Capacity**"). Unused Service Capacity will not roll over to any future Subscription Terms. If Customer's actual usage of the Services during the Subscription Term exceeds the Service Capacity, Customer will be charged for the excess usage at the rates set forth in the applicable Order Form without any discounts.

3.3 Unless otherwise stated, Klarity's fees do not include any taxes, levies, duties or similar governmental assessments of any nature, including but not limited to value-added, sales and use, or withholding taxes, assessable by any local, state, provincial, federal or foreign jurisdiction (collectively, "**Taxes**"). Customer is responsible for paying all Taxes associated with its purchases hereunder. If Klarity has the legal obligation to pay or collect Taxes for which Customer is responsible under this paragraph, the appropriate amount will be invoiced to and paid by Customer, unless Customer provides Klarity with a valid tax exemption certificate authorized by the appropriate taxing authority. For clarity, Klarity is solely responsible for taxes assessable against it based on its income, property and employees.

4. CONFIDENTIALITY

4.1 Each party (the "**Receiving Party**") understands that the other party (the "**Disclosing Party**") has disclosed or may disclose business, technical or financial information relating to the Disclosing Party's business (hereinafter referred to as "**Confidential Information**" of the Disclosing Party). Confidential Information of Klarity includes non-public information regarding features, functionality and performance of the Services. Customer's Confidential Information includes Customer Data (as defined in the AI Addendum). The

Receiving Party agrees: (i) to take reasonable precautions to protect such Confidential Information, and (ii) not to use (except in performance of the Services or as otherwise permitted herein) or divulge to any third person any such Confidential Information other than its representatives. The Disclosing Party agrees that the foregoing will not apply with respect to any Confidential Information after five (5) years following the disclosure thereof or any information that (a) is or becomes publicly available without breach of this Agreement by the Receiving Party or any of its representatives; (b) was in the possession of the Receiving Party or any of its representatives prior to disclosure hereunder; (c) is lawfully acquired by the Receiving Party or any of its representatives from a source not known by the Receiving Party or such representative to have violated any contractual or legal obligation of confidentiality to the Disclosing Party in its disclosure of such information, or (d) is or was independently developed by the Receiving Party or any of its representatives without use of or reference to any Confidential Information. Confidential Information may be disclosed if required by applicable law, in which case the Receiving Party will, unless prohibited by applicable law, provide prompt prior written notice to the Disclosing Party and will limit such disclosure to only that information which must be disclosed.

5. TERM AND TERMINATION

5.1 This Agreement is for the Initial Subscription Term as specified in the Order Form and all Subscription Terms under individual Order Forms entered into between Customer and Klarity on or after the date hereof. Each Order Form will automatically renew for additional successive 12-month periods unless either party gives written notice of non-renewal at least thirty (30) days before the end of the then-current Subscription Term.

5.2 Either party may terminate this Agreement if the other party (i) materially breaches any terms and conditions of this Agreement and does not cure such breach within thirty (30) days of receiving notice of such breach; or (ii) becomes the subject of a petition in bankruptcy or any proceeding relating to insolvency, receivership, liquidation or assignment for the benefit of creditors. If Customer terminates this Agreement for material breach, Klarity agrees to promptly refund to Customer any pre-paid fees, pro-rated for the remainder of the term of this Agreement.

5.3 Termination of this Agreement will terminate any outstanding Order Forms. All sections of this Agreement which by their nature should survive termination will survive termination, including, without limitation, accrued rights to payment, confidentiality obligations, warranty disclaimers, limitations of liability, and indemnification.

6. CUSTOMER'S RIGHTS AND RESPONSIBILITIES

6.1 Customer will retain ownership of all Customer Confidential Information, including but not limited to Customer Data.

6.2 Customer will not, directly or indirectly: reverse engineer, decompile, disassemble or otherwise attempt to discover the source code, object code or underlying structure, ideas, know-how or algorithms relevant to the Services or any software, documentation or data related to the Services; modify, translate, or create derivative works based on the Services (except to the extent expressly permitted by Klarity or authorized within the Services); copy any features, functions or graphics of the Services; permit any third party to access the Services except as permitted herein or in an Order Form; publish any benchmarking results relating to the Services; access or use the Services for any purpose other than its own internal use; use the Services for timesharing or service bureau purposes or otherwise for the benefit of a third party; or remove any proprietary notices or labels.

6.3 Customer will be responsible for obtaining and maintaining any equipment and ancillary services required to access and use the Services, including, without limitation, modems, hardware, servers, software, operating systems, networking, web servers and the like (collectively, "**Equipment**"). Customer will also be responsible for maintaining the security of the Equipment, and for all uses of the Equipment with or without Customer's knowledge or consent.

6.4 Customer and Users will use the Services only in compliance with all applicable laws and regulations and this Agreement. Customer and Users will not use the Services to store or transmit infringing, libelous, or otherwise unlawful or tortious material or information. If Customer becomes aware of any violation of Customer's obligations under this Agreement by any User, Customer will promptly notify Klarity.

7. KLARITY'S RIGHTS AND RESPONSIBILITIES

7.1 Klarity will own and retain all right, title and interest in and to (a) the Services, all improvements, enhancements or modifications thereto, (b) any software, applications, inventions or other technology developed in connection with the Services and technical support services, and (c) any suggestions, enhancement requests, recommendations or other feedback provided by Customer, including Users, relating to the Services or technical support services ("**Feedback**") provided that Feedback will not contain any Insulated Information (as defined in the AI Addendum).

7.2 Klarity may (i) collect and analyze information relating to the provision, use and performance of the Services and related systems and technologies ("**Usage Data**"), (ii) use Usage Data to improve and enhance the Services and for other development, diagnostic and corrective purposes in connection with the Services and other Klarity offerings, and (iii) disclose Usage Data solely in aggregate or other anonymized, unidentifiable form in connection with its business, provided that Usage Data will not contain any Insulated Information.

7.3 Klarity will have the right to monitor Customer's use of the Services to verify compliance with this Agreement. Klarity may also use the Services to perform such monitoring and enforce the restrictions on Customer's use of the Services herein.

8. WARRANTY AND DISCLAIMER

8.1 Each party represents and warrants to the other that it has the full authority and power to enter into and perform its obligations under this Agreement, and that the execution and performance of this Agreement does not and will not conflict with or violate any agreement, order or legal process to which such party is subject, nor require the consent of any government authority, corporation, limited liability company, partnership, organization, association or other legal entity.

8.2 Klarity warrants to Customer that the Services will operate substantially in accordance with its documentation. Klarity will use reasonable efforts consistent with prevailing industry standards to maintain the Services in a manner which minimizes errors and interruptions in the Services and will perform onboarding services in a professional and workmanlike manner. Services may be temporarily unavailable for scheduled maintenance or for unscheduled emergency maintenance, either by Klarity or by third-party providers, or because of other causes beyond Klarity's reasonable control, but Klarity will use reasonable efforts to provide advance notice in writing (e-mail sufficient) of any scheduled service disruption. Although several Klarity employees and contractors are licensed attorneys and CPAs, Klarity is not a law firm, an accounting firm or a tax firm, is not engaged in the practice of law, accounting or tax services, and under no circumstance is an attorney-client relationship formed between Klarity and Customer and any of Customer clients (if applicable). Klarity work-product will not constitute legal opinions or legal advice and are prepared at the direction of, and for review by, Customer. Customer agrees that it is its sole responsibility to ensure the accuracy and completeness of the final product. Customer's sole remedy for a breach of any warranty set forth in this Agreement will be as provided in the "Term and Termination" section of this Agreement. HOWEVER, KLARITY DOES NOT WARRANT THAT THE SERVICES WILL BE UNINTERRUPTED OR ERROR FREE; NOR DOES IT MAKE ANY WARRANTY AS TO THE RESULTS THAT MAY BE OBTAINED FROM USE OF THE SERVICES. EXCEPT AS EXPRESSLY SET FORTH IN THIS SECTION, THE SERVICES AND ONBOARDING SERVICES ARE PROVIDED "AS IS" AND COMPANY DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.

9. LIMITATION OF LIABILITY

9.1 EXCEPT FOR BODILY INJURY OF A PERSON, NEITHER PARTY NOR ITS SUPPLIERS (INCLUDING BUT NOT LIMITED TO EQUIPMENT AND TECHNOLOGY SUPPLIERS), OFFICERS, AFFILIATES, REPRESENTATIVES, CONTRACTORS AND EMPLOYEES WILL BE RESPONSIBLE OR LIABLE WITH RESPECT TO ANY SUBJECT MATTER OF THIS AGREEMENT UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER THEORY: (A) FOR ERROR OR INTERRUPTION OF USE OR FOR LOSS OR INACCURACY OR CORRUPTION OF DATA OR COST OF PROCUREMENT OF SUBSTITUTE GOODS, SERVICES OR TECHNOLOGY OR LOSS OF BUSINESS; (B) FOR ANY INDIRECT, EXEMPLARY, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES; (C) FOR ANY MATTER BEYOND A PARTY'S REASONABLE CONTROL; OR (D) FOR ANY AMOUNTS THAT, TOGETHER WITH AMOUNTS ASSOCIATED WITH ALL OTHER CLAIMS, EXCEED THE FEES PAID BY CUSTOMER TO KLARITY FOR THE SERVICES UNDER THIS AGREEMENT IN THE 12 MONTHS PRIOR TO THE ACT THAT GAVE RISE TO THE LIABILITY, IN EACH CASE, WHETHER OR NOT SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. NOTWITHSTANDING THE FOREGOING, NO LIMITATION OR EXCLUSION OF LIABILITY WILL APPLY WITH RESPECT TO ANY CLAIMS BASED ON BREACH OF CONFIDENTIALITY OR ON FRAUD, GROSS NEGLIGENCE OR WILLFUL MISCONDUCT.

10. INDEMNITY

10.1 Klarity will defend and indemnify Customer and its Affiliates from and against all losses, damages, liabilities, costs, and expenses (including reasonable attorneys' fees) arising out of a third party claim, action or proceeding alleging that the Services, or the use thereof as permitted by this Agreement, infringes or otherwise violates any intellectual property rights or applicable law.

10.2 Customer will defend and indemnify Klarity and its Affiliates from and against all losses, damages, liabilities, costs, and expenses (including reasonable attorneys' fees) arising out of a third party claim, action or proceeding alleging that Customer's or a User's use of the Services in violation of this Agreement infringes or otherwise violates any intellectual property rights or applicable law.

10.3 The indemnified party will give the indemnifying party prompt written notice of any claim. The indemnifying party has the right to

control the defense or settlement of the claim; provided, however, that the indemnifying party may not settle any claim if it imposes any liability or obligation on the indemnified party or its Affiliates without the indemnified party's prior written consent. This "Indemnification" section states the indemnifying party's sole liability to, and the indemnified party's exclusive remedy against, the other party for any type of claim, action or proceeding described in this section.

11. MISCELLANEOUS

11.1 All notices under this Agreement will be in writing and will be deemed to have been duly given when received, if personally delivered; when receipt is electronically confirmed, if transmitted by email; the day after it is sent, if sent for next day delivery by recognized overnight delivery service; and upon receipt, if sent by certified or registered mail, return receipt requested.

11.2 This Agreement may be executed in counterparts, which taken together will form one legal instrument. If any provision of this Agreement is found to be unenforceable or invalid, that provision will be limited or eliminated to the minimum extent necessary so that this Agreement will otherwise remain in full force and effect and enforceable. This Agreement is the complete and exclusive statement of the mutual understanding of the parties and supersedes and cancels all prior and contemporaneous written and oral agreements, communications and other understandings relating to the subject matter of this Agreement. All waivers and modifications must be in a writing signed by both parties, except as otherwise provided herein. However, to the extent of any conflict or inconsistency between the provisions in the body of this Agreement and any exhibit or addendum hereto or any Order Form, the terms of such exhibit, addendum or Order Form will prevail. Notwithstanding any language to the contrary therein, no terms or conditions stated in a Customer purchase order or in any other Customer order documentation (excluding Order Forms) will be incorporated into or form any part of this Agreement, and all such terms or conditions will be null and void.

11.3 The parties are independent contractors. No agency, partnership, joint venture, fiduciary or employment is created as a result of this Agreement and Customer does not have any authority to bind Klarity whatsoever. In any action relating to this Agreement, the prevailing party will be entitled to recover costs and attorneys' fees.

11.4 Klarity may, in its discretion, use Klarity Affiliates and/or subcontract third parties (each a "**Klarity Subcontractor**"), in each case within or outside of the United States. Klarity may provide information relevant to this Agreement to Klarity Affiliates and/or Klarity Subcontractors for the Services and/or for internal administrative and regulatory compliance purposes. All information will be shared subject to the confidentiality provisions in this Agreement. Klarity will be solely responsible for the provision of the Services (including those performed by Klarity Affiliates or Klarity Subcontractors).

11.5 Neither party may assign this Agreement without the other party's prior written consent, which consent will not be unreasonably withheld or delayed; provided, however, that a party may assign this Agreement (a) to any Affiliate; (b) in connection with a merger or sale of all or substantially all of its stock or assets; or (c) in connection with any divestiture or spin-off of any entity or division, business unit or department within an entity. Any other purported assignment will be void. This Agreement will bind and inure to the benefit of the parties, their respective successors and permitted assigns.

11.6 Neither party will be liable for or considered in breach of or default under this Agreement on account of any delay or failure to perform as required by this Agreement as a result of fire, strike, war, terrorism, insurrection, government restriction or prohibition, pandemic disease, or any other causes or conditions which are beyond such party's reasonable control and which such party is unable to overcome by the exercise of reasonable diligence.

11.7 Subject to Customer's prior consent, Klarity may use Customer's name and logo for marketing purposes and generally refer to Customer as Klarity's customer. If Customer grants such consent, Klarity will enjoy a limited license to certain specified copyrighted material and/or trademarks that protect Customer's logo.

11.8 This Agreement will be governed by the laws of California without regard to its conflict of law provisions. All disputes and legal proceedings related to this Agreement will be maintained in state and federal courts located in California and the parties consent to the personal jurisdiction of such courts. Each party waives any right to jury trial in connection with any action or litigation in any way arising out of or related to this Agreement.

EXHIBIT A
SERVICE LEVEL AGREEMENT

This Service Level Agreement ("**SLA**") forms a part of and is subject to the Agreement.

1. Customer Support. Klarity will provide Technical Support to Customer via both telephone and e-mail on weekdays during the hours of 8 am through 5 pm Pacific time, with the exclusion of Federal Holidays ("**Support Hours**"). Customer may initiate a helpdesk ticket during Support Hours by calling (617) 913-9300 or any time by opening a chat window in Klarity Services. Klarity guarantees response time as per Support level included in the then-current Order Form accompanying the Agreement.

2. System Uptime Availability. During the Subscription Term, the Services will be available 99.7% ("**Target Availability Percentage**"), measured monthly, excluding holidays, weekends and scheduled maintenance. Service Level Terms for other Customer contracts will be separately agreed upon by the parties. If Customer requests maintenance during the available hours, any uptime calculation will exclude periods affected by such maintenance. Further, any downtime resulting from outages of third party connections or utilities or other reasons beyond Klarity's control will also be excluded from any such calculation.

3. System Uptime Service Credits. If during any calendar month of the Subscription Term, the Availability Percentage is lower than the Target Availability Percentage, and Customer notifies Klarity about the Downtime within 30 days of its occurrence in writing, Klarity will provide Customer with a credit for any verified Downtime (the "**Service Credit**") as follows:

Availability Percentage	95% - 99.6%	90%-94.9%	85%-89.9%	below 85%
Service Credit	5% Monthly Subscription Fee	10% Monthly Subscription Fee	20% Monthly Subscription Fee	25% Monthly Subscription Fee

4. Service Credit Terms. Failure to provide such written notice will forfeit the right to receive Service Credits. Service Credits may not be redeemed for cash and constitute liquidated damages, not a penalty. Klarity will only apply a credit to the month in which the incident occurred. If Customer is current on its payment obligations, then Klarity will apply Service Credits to Customer's next invoice. If Customer is not current on its payment obligations, then Klarity will apply Service Credits after Customer pays up any owed amount in full. If Customer will not receive a future invoice because their Subscription Term will not renew, Klarity will extend Customer's then-current Subscription Term for a period of time corresponding to the amount of the credit (e.g. 5% Service Credit equals 5% Calendar Month extension). Service Credits are Customer's sole remedy (and Klarity's sole liability) for Klarity Service Availability failures. Simultaneous Availability events (e.g. simultaneous Uptime and Load Time failures) do not accrue duplicate Service Credits. In no event will Service Credits in any Calendar Month exceed 25% of total Monthly Fees for that Calendar Month in case of System Uptime Availability.

EXHIBIT B
DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") forms a part of the Agreement between Klarity and Customer for the provision of Services by Klarity to Customer and applies to Klarity's Processing of Personal Data (as defined below) provided by Customer to Klarity as part of Klarity's provision of Services under the Agreement. The terms of this DPA will be effective and replace any previously applicable data processing terms as of the date of last signature.

1. Definitions.

a. "**Business**," "**Business Purpose**," "**Consumer**," "**Person**," "**Personal Information**," "**Sell**," "**Service Provider**," and "**Third Party**" have the meanings set forth in U.S. Data Protection Law.

b. "**Controller**", "**Processor**", "**Data Subject**", "**Personal Data**" and "**Processing**" (and "**Process**") have the meanings given in Applicable Data Protection Law.

c. "**Applicable Data Protection Law**" will mean: (i) Regulation 2016/679 of the European Parliament and of the Council 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); (ii) EU Directive 2002/58/EC concerning the Processing of Personal Data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications); (iii) U.S. Data Protection Law; (iv) any state or national legislation made under or pursuant to (i), (ii), or (iii); (v) any amendments or successor legislation to (i), (ii), (iii), or (iv); and (vi) any other applicable data protection law.

d. "**U.S. Data Protection Law**" means all laws and regulations of the United States of America, including the California Consumer Privacy Act of 2018, applicable to the processing of "Personal Information" (or an analogous variation of such term).

2. Relationship of the parties; Limitations on Processing. Customer is the Controller of the Personal Data that is the subject matter of the Agreement ("**Data**") and appoints Klarity as a Processor to Process such Data. Each party will comply with the obligations that apply to it under Applicable Data Protection Law. Klarity will Process the Data as a Processor only as necessary to perform its obligations under the Agreement and in accordance with the documented instructions of Customer (the "**Permitted Purpose**"), except where otherwise required by Applicable Data Protection Law. In no event will Klarity Process the Data for its own purposes or those of any third party except as set forth in the Agreement. Klarity will ensure that any person it authorizes to Process the Data ("**Authorized Person**") Processes the Data only as necessary for the Permitted Purpose and is subject to a duty of confidentiality requiring them to keep such Data confidential.

3. International Transfers. Klarity will not transfer the Data (nor permit the Data to be transferred) outside of the European Economic Area ("**EEA**") unless (i) it has first obtained Customer's prior written consent; and (ii) enters into the standard contractual clauses for the transfer of personal data from these jurisdictions to processors established in third countries - as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 ("**Standard Contractual Clauses**") attached hereto. Klarity will not transfer the Data (nor permit the Data to be transferred) outside of the United Kingdom unless (i) it has first obtained Customer's prior written consent; and (ii) enters into the standard contractual clauses for the transfer of personal data from the United Kingdom to processors established in third countries ("**UK Standard Contractual Clauses**") attached hereto.

4. Security. Klarity will implement appropriate technical and organizational measures to protect the Data (i) from accidental or unlawful destruction, and (ii) loss, alteration, unauthorized disclosure of, or access to the Data, and (iii) any act or omission that compromises either the security, confidentiality, or integrity of the Data or the physical, technical, administrative, or organizational safeguards put into place by Klarity (a "**Security Incident**"). Such measures will have regard to 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. Klarity's Processing of the Data will comply with all Applicable Data Protection Law. Klarity will implement and maintain a written information security program, including appropriate policies, procedures, and risk assessments that are reviewed at least annually. Such measures may include, as appropriate: (i) the anonymization and encryption of the Data; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services; (iii) the ability to restore the availability and access to the Data in a timely manner in the event of a Security Incident; and (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

5. Security Incidents. Upon becoming aware of a Security Incident, Klarity will inform Customer within 48 hours and will provide all such timely information and cooperation as Customer may require in order for Customer to fulfill its data breach reporting obligations under Applicable Data Protection Law. Klarity will further take all such measures and actions as are necessary to remedy or mitigate the effects of the Security Incident and will keep Customer apprised of all developments in connection with the Security Incident. Klarity agrees that it

will not inform any third party of any Security Incident without first obtaining Customer's prior written consent, other than to inform a complainant that the matter has been forwarded to Customer's legal counsel or as required by Applicable Data Protection Law. Further, Klarity agrees that except as required by Applicable Data Protection Law Customer will have the sole right to determine: (i) whether notice of the Security Incident is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies, or others as required by law or regulation, or otherwise in Customer's discretion, and (ii) the contents of such notice, whether any type of remediation may be offered to affected persons, and the nature and extent of any such remediation.

6. Subprocessing. Customer authorizes the engagement of Klarity's Affiliates as subprocessors. Customer authorizes Klarity to engage third party subprocessors to Process the Data provided: (i) Klarity notifies Customer in writing (email sufficient), (ii) Klarity imposes data protection terms on any subprocessor substantially similar terms to the terms of this DPA; and (iii) Klarity remains fully liable for any breach of this DPA that is caused by an act, error or omission of its subprocessor. Customer may object to Klarity's appointment of a third party subprocessor within thirty (30) days after receiving Klarity's notification, provided such objection is on reasonable grounds relating to the protection of the Data. In such an event, Klarity will either not appoint or replace the subprocessor or, if this is not possible, Customer may suspend or terminate this DPA. Customer authorizes Klarity to use the subprocessors listed in Annex 3 to the Standard Contractual Clauses attached hereto.

7. Cooperation and Data Subjects' Rights. Klarity will provide all reasonable and timely assistance (including by appropriate technical and organizational measures) to Customer to enable Customer to respond to: (i) any request from a Data Subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a Data Subject, regulator or other third party in connection with the Processing of the Data. In the event that any such request, correspondence, enquiry or complaint is made directly to Klarity, Klarity will promptly inform Customer providing details of the same.

8. Deletion of Data. Upon Customer's written request, Klarity will delete all Data in its possession or control. This requirement will not apply to the extent Klarity is required by Applicable Data Protection Law to retain the Data, in which event Klarity will protect the Data from any further Processing except to the extent required by such law.

9. CCPA Compliance. Customer is a Business and appoints Klarity as a Service Provider to process certain Personal Information on behalf of Customer ("**Customer Personal Information**"). Except as provided in this DPA, Customer will not Sell the Customer Personal Information to Klarity and Klarity will not Sell the Customer Personal Information. Unless otherwise required by law, Klarity will not retain, use or disclose the Customer Personal Information other than for the specific purpose of providing the Services and as part of the direct relationship between Klarity and Customer.

10. Audit. Klarity will permit upon Customer's written request, when Customer has reasonable cause to believe Klarity is in non-compliance with its obligations under this DPA, a mutually agreed-upon third party auditor (the "**Auditor**") to audit Klarity's compliance with this DPA and will make available to such third-party auditor all information, systems and staff necessary for the Auditor to conduct such audit. Klarity acknowledges that the Auditor may enter its premises for the purposes of conducting this audit, provided that Customer gives it reasonable prior notice of its intention to audit, conducts its audit during normal business hours, and takes all reasonable measures to prevent unnecessary disruption to Klarity's operations. Customer will not exercise its audit rights more than once in any twelve (12) calendar month period, except: (i) if and when required by Applicable Data Protection Law or instruction of a competent data protection authority; (ii) Customer reasonably believes a further audit is necessary due to a Security Incident suffered by Klarity, or (iii) as mutually agreed between the parties.

11. Mandatory Disclosure. Klarity may disclose this DPA and any relevant privacy provisions in the Agreement to the US Department of Commerce, the Federal Trade Commission, European data protection authority, or any other U.S. or EU judicial or regulatory body upon their request and that any such disclosure will not be deemed a breach of the Agreement or this DPA. Notwithstanding anything in the Agreement or this DPA to the contrary, Klarity may cooperate with law enforcement agencies concerning conduct or activity that it reasonably and in good faith believes may violate international, federal, state, or local law.

EXHIBIT C
STANDARD CONTRACTUAL CLAUSES FOR THE TRANSFER OF PERSONAL DATA

Customer, as specified in the Terms of Service with address, telephone and fax number and email contact information, as "**data exporter**", and Klarity Intelligence, Inc., as defined in the Data Processing Addendum, as "**data importer**", each a "party"; together "the parties", have agreed on the provisions above and the following Standard Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

SECTION I

Clause 1: **Purpose and scope**

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) ([1]) for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2: **Effect and invariability of the Clauses**

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3: **Third-party beneficiaries**

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:: (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7; (ii) Clause 8.1(b), 8.9(a), (c), (d) and (e); (iii) Clause 9(a), (c), (d) and (e); (iv) Clause 12(a), (d) and (f);(v) Clause 13; (vi) Clause 15.1(c), (d) and (e); (vii) Clause 16(e); (viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4: **Interpretation**

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms will have the same meaning as in that Regulation.

(b) These Clauses will be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses will not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5: **Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses will prevail.

Clause 6: **Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7: **Docking clause**

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity will become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity will have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II: OBLIGATIONS OF THE PARTIES

Clause 8: **Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer will process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer will immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer will process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter will make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but will provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties will provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it will inform the data exporter without undue delay. In this case, the data importer will cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer will only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer will, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer will continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter will implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties will take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties will in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject will, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer will at least implement the technical and organisational measures specified in Annex II. The data importer will carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer will grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It will ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer will take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer will also notify the data exporter without undue delay after having become aware of the breach. Such notification will contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification will contain the information then available and further information will, as it becomes available, subsequently be provided without undue delay.

(d) The data importer will cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer will apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer will only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([2]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

8.9 Documentation and compliance

(a) The data importer will promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties will be able to demonstrate compliance with these Clauses. In particular, the data importer will keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer will make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and will, where appropriate, be carried out with reasonable notice.

(e) The Parties will make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

***Clause 9*: Use of sub-processors**

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer will specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 7 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer will provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it will do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([3]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer will ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer will provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer will remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer will notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer will agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter will have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

***Clause 10*: Data subject rights**

(a) The data importer will promptly notify the data exporter of any request it has received from a data subject. It will not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer will assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties will set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance will be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer will comply with the instructions from the data exporter.

***Clause 11*: Redress**

(a) The data importer will inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It will deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

compliance with these Clauses, that Party will use its best efforts to resolve the issue amicably in a timely fashion. The Parties will keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer will accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer will abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

***Clause 12*: Liability**

(a) Each Party will be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer will be liable to the data subject, and the data subject will be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter will be liable to the data subject, and the data subject will be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it will be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties will be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it will be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

***Clause 13:* Supervision**

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, will act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, will act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, will act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It will provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III: LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

***Clause 14:* Local laws and practices affecting compliance with the Clauses**

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([4]);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter will promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter will suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter will be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) will apply.

***Clause 15:* Obligations of the data importer in case of access by public authorities**

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification will include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification will include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer will, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer will seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It will not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It will also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

***Clause 16:* Non-compliance with the Clauses and termination**

(a) The data importer will promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter will suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter will be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it will inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) will at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same will apply to any copies of the data. The data importer will certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer will continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

***Clause 17*: Governing law**

These Clauses will be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this will be the law of Ireland.

***Clause 18*: Choice of forum and jurisdiction**

(a) Any dispute arising from these Clauses will be resolved by the courts of an EU Member State. The Parties agree that those will be the courts of Ireland.

(b) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(c) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX 1 TO THE STANDARD CONTRACTUAL CLAUSES
PARTIES AND DETAILS OF PROCESSING

A. LIST OF PARTIES

Data exporter
The data exporter is Customer or its employees or affiliates.
Name: Customer as specified in the Agreement
Address:
Contact person's name, position and contact details:
Activities relevant to the data transferred under these Clauses: as per the Agreement, the DPA and this Annex 1
Signature and date: As set forth in the DPA
Role (controller/processor): Controller

Data importer
The data importer is Klarity Intelligence, Inc.
Name: Klarity Intelligence, Inc.
Address: As specified in the Agreement
Contact details: infosec@klarity.ai
Activities relevant to the data transferred under these Clauses: as per the Agreement, the DPA and this Annex 1
Signature and date: As set forth in the DPA
Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred
The personal data transferred concern data subjects residing in the European Economic Area and Switzerland.

Categories of personal data transferred
The personal data transferred concern the following categories of data:
Data exporter may transfer Personal Data to data importer, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, and is not limited to the following categories of personal data:

- First and last name
- Contact information (telephone number & email address)
- Company, position
- Login credentials

Special categories of data (if appropriate)
None

Processing operations
The objective of the processing of personal data by data importer is the access and use of Klarity Services.

Notification Obligation
If Klarity begins collecting additional categories of data or changes the processing operations it will immediately notify data exporter to modify or amend this Appendix.

The frequency of the transfer
A continuous basis for the duration of the Agreement in accordance with the terms of the DPA.

Nature of the processing
Klarity will Process the Data as in accordance with the terms of the Agreement and the DPA.

Purpose(s) of the data transfer and further processing
Klarity will Process the Data as a Processor only as necessary to perform its obligations under the Agreement, and strictly in accordance with the Permitted Purpose, except where otherwise required by any applicable EU (or any EU Member State) law. In no event will Klarity Process the Data for its own purposes or those of any third party except as set forth in the Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
Until deletion in accordance with the provisions of the DPA.

For transfers to (sub-)processors, also specify subject matter, nature and duration of the processing
As described in the DPA.

C. COMPETENT SUPERVISORY AUTHORITY

Location of data exporter	***Supervisory Authority***
Data exporter is established in an EU Member State	The Data Protection Commission of Ireland
Data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of GDPR.	The Data Protection Commission of Ireland
Data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of GDPR.	The Data Protection Commission of Ireland

ANNEX 2 TO THE STANDARD CONTRACTUAL CLAUSES
TECHNICAL AND ORGANISATIONAL MEASURES

Measures of pseudonymisation and encryption of personal data
Klarity will maintain a written information security program, including appropriate policies, procedures, and risk assessments that are reviewed at least annually. Such measures may include, as appropriate, the anonymization and encryption of the Data. Klarity maintains the Data in an encrypted format in transit (HTTPS/TLS) and at rest (AES-256).

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
Klarity will implement and maintain a written information security program, including appropriate policies, procedures, and risk assessments that are reviewed at least annually, including appropriate technical and organizational measures to protect the Data from a Security Incident. Such measures will have regard to 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. Such measures may include, as appropriate: (i) the anonymization and encryption of the Data; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services; (iii) the ability to restore the availability and access to the Data in a timely manner in the event of a physical or technical incident; (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
Klarity will implement and maintain a written information security program, including appropriate policies, procedures, and risk assessments that are reviewed at least annually. Such measures may include, as appropriate, the ability to restore the availability and access to the Data in a timely manner in the event of a physical or technical incident. Klarity performs regular backups of the Data, which is hosted in AWS data centers. Backups are retained redundantly across multiple availability zones.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing
Klarity will implement and maintain a written information security program, including appropriate policies, procedures, and risk assessments that are reviewed at least annually. Such measures may include, as appropriate, to Process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing. Klarity maintains a risk-based assessment security program. The framework for Klarity's security program includes administrative, organizational, technical, and physical safeguards reasonably designed to protect the Services and confidentiality, integrity, and availability of the Data.

Measures for user identification and authorization
Klarity personnel are required to use unique user access credentials and passwords for authorization. Klarity follows the principles of least privilege through role-based and time-based access models when provisioning system access. Access is promptly removed upon role change or termination.

Measures for the protection of data during transmission
Klarity will ensure that any person that it authorizes to Process the Data including Klarity's Authorized Persons will be subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty) and will not permit any person to Process the Data who is not under such a duty of confidentiality. Klarity will ensure that all Authorized Persons Process the Data only as necessary for the Permitted Purpose. Klarity will not transfer the Data (nor permit the Data to be transferred) outside of the EEA unless (i) it has first obtained Customer's prior written consent; and (ii) enters into the Standard Contractual Clauses attached hereto.

Measures for the protection of data during storage
The Data is stored encrypted using AES-256.

Measures for ensuring physical security of locations at which personal data are processed
The Services operate on Amazon Web Services ("**AWS**") and are protected by the security controls of AWS.

Measures for ensuring events logging
Klarity monitors access to applications, tools, and resources that process or store Data, including cloud services. Monitoring of security logs is centralized by the security team.

Measures for ensuring system configuration, including default configuration
New account configurations are approved by each customer. Klarity adheres to a change management process to administer changes to the production environment for the Services, including changes to its underlying software, applications, and systems. The Klarity system

maintains an audit trail of all changes to contract review rules and account settings. Changes to contract review rules are initiated by the customer and restricted to authorized personnel.

Measures for internal IT and IT security governance and management
Biannual security meetings are held with the entire company and are led by the CTO to review all information security policies and to communicate specific security related topics. Klarity's enterprise Mobile Device Management solution, Rippling, is installed on all employee workstations. Amongst other things, it allows for password complexity enforcements, encryption enforcement and remote locking/wiping. VPN connection is required in order for employees to access all internal IT systems. Separate VPN connections are required for the Production and QA environments. User access to systems and data is based on the "Principle of Least Privilege", wherein users are given only the minimum amount of access privileges required to satisfy their role. Passwords to all IT systems (including employee workstations) follow these rules: password length must be at least 32 characters. Passwords and IT system credentials are stored only on Bitwarden, Klarity's self-hosted password management system. Wherever possible (and particularly with systems with access to live customer data) multi-factor authentication must be enabled when logging into IT systems. All employees are required to complete a security awareness seminar immediately upon joining and twice a year thereafter.

Measures for certification/assurance of processes and products
Klarity is SOC 1 Type II and SOC 2 Type II certified. Penetration tests are conducted after any major changes to the system's functionality, however, not less than annually.

Measures for ensuring data minimization
When setting up integrations, Klarity recommends the following best practices to customers to minimize data transfer: restricting the access of the Klarity API user to "Read" permissions for only the objects and metadata fields Klarity will need to import and (ii) configuring triggers/webhooks within the source application as narrowly as possible so that Klarity is only notified of documents it needs to process and nothing additional.

Measures for ensuring data quality
New customer accounts are approved by management prior to account set up and based upon customer specifications within the business requirements agreement. Klarity performs manual annotation and validates results against system results before production go-live. The information system is reviewed at a defined frequency to identify and eliminate unnecessary functions, ports, protocols, and/or services.

Measures for ensuring limited data retention
Upon Customer's written request, Klarity will delete all Data in its possession or control. This requirement will not apply to the extent Klarity is required by Applicable Data Protection Law to retain some or all of the Data, in which event Klarity will isolate and protect the Data from any further Processing except to the extent required by such law.

Measures for ensuring accountability
Compliance to infosec policies is tracked centrally through Vanta (SOC 2 compliance), Avast Pro Plus (Antivirus) and Rippling (MDM). All infosec policies detail consequences for violation, administered by the CTO.

Measures for allowing data portability and ensuring erasure
Klarity maintains a comprehensive list of locations containing customer data, as well as scripts that systematically delete customer data from said locations when needed. Production and QA environments are completely logically separated from each other. No customer data is ever stored in any non-Production environment.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter
Customer authorizes Klarity to engage third party subprocessors to Process the Data provided: (i) Klarity notifies Customer in writing (email sufficient), (ii) Klarity imposes data protection terms on any subprocessor substantially similar terms to the terms of this DPA; and (iii) Klarity remains fully liable for any breach of this DPA that is caused by an act, error or omission of its subprocessor. Customer may object to Klarity's appointment of a third party subprocessor within thirty (30) days after receiving Klarity's notification, provided such objection is on reasonable grounds relating to the protection of the Data. In such event, Klarity will either not appoint or replace the subprocessor or, if this is not possible, Customer may suspend or terminate this DPA.

ANNEX 3 TO THE STANDARD CONTRACTUAL CLAUSES
LIST OF SUBPROCESSORS

Customer specifically consents to Klarity using the following subprocessors as forth in the DPA:

Name	Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised)
Amazon Web Services, Inc.	Klarity's infrastructure is entirely hosted on AWS.
MongoDB, Inc.	Klarity uses MongoDB's database hosted on AWS for storage of data points extracted from contracts.
Asana, Inc.	Klarity uses Asana to track customer feature requests and bug reports that often include personal data of customer's employees who submitted such requests. Klarity does not store any contracts or other documents containing personal data in Asana.
Google LLC	Klarity uses Google to communicate with customers and in its document processing pipeline.
Slack Technologies, LLC	Klarity uses Slack for Customer support.
Elasticsearch, B.V.	For customers who choose to use our optional analytics module, Klarity Analytics will be hosted on Elastic Cloud (using AWS for underlying storage).
Khosla Labs Pvt. Ltd.	Khosla Labs is Klarity's long-term provider of implementation and annotation services headquartered in Bangalore, India. Klarity has had a long-term contract with Khosla Labs since 2017.
Microsoft Corporation	Klarity uses Microsoft Azure for tabular extractions.
Workato, Inc.	Workato's platform helps Klarity build integrations with third-party applications.
ZoomInfo Technologies Inc.	Klarity uses ZoomInfo's Chorus product for recording calls and structuring next steps to ensure that context is effectively transferred within the Klarity team.
OpenAI, L.P.	Klarity uses OpenAI's GPT product to perform document extractions, computations and interactions.
Pinecone Systems, Inc.	Klarity uses Pinecone to store text embeddings vectors (sets of numbers that represent document text) as well as related document text and metadata.
Okta, Inc.	Klarity uses Okta for Single Sign On (SSO) services.
Connor Group Global Services, LLC	Klarity uses Connor Group for advisory and technology services to support client's integrations and implementations, leveraging Klarity's or client's iPaaS solutions.
Gong.io Inc.	Klarity uses Gong to record calls.
Anthropic PBC	Klarity uses Anthropic products in its document processing pipeline.

ANNEX 4 TO THE STANDARD CONTRACTUAL CLAUSES
INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU STANDARD CONTRACTUAL CLAUSES

PART 1: PARTIES

Table 1: Parties

Start date	As defined in the Agreement	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Customer, as defined in the Agreement	Klarity, as defined in the Agreement
Key Contact	Full Name (optional): Job Title: Contact details including email:	Contact details including email: infosec@klarity.ai

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, including the Appendix Information

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: Please refer to the **Agreement** and the **DPA**.

Annex 1B: Description of Transfer: **Annex 1 to the Standard Contractual Clauses**

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: **Annex 2 to the Standard Contractual Clauses**

Annex III: List of Sub processors (Modules 2 and 3 only): **Annex 3 to the Standard Contractual Clauses**

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: Importer

PART 2: MANDATORY CLAUSES

Entering into this Addendum

Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

Where this Addendum uses terms that are defined in the Approved EU SCCs those terms will have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.

UK GDPR	As defined in section 3 of the Data Protection Act 2018.

1. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
2. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.
3. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.
4. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
5. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

1. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.
2. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.
3. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

1. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
2. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
3. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
4. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.
5. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.
6. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.
7. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:
8. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;
9. In Clause 2, delete the words:

i. "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

10. Clause 6 (Description of the transfer(s)) is replaced with:

i. "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

11. Clause 8.7(i) of Module 1 is replaced with:

i. "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

12. Clause 8.8(i) of Modules 2 and 3 is replaced with:

i. "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

13. References to "Regulation (EU) 2016/679", "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 (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;
14. References to Regulation (EU) 2018/1725 are removed;
15. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";
16. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";
17. Clause 13(a) and Part C of Annex I are not used;
18. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";
19. In Clause 16(e), subsection (i) is replaced with:

i. "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

20. Clause 17 is replaced with:

i. "These Clauses are governed by the laws of England and Wales.";

21. Clause 18 is replaced with:

i. "Any dispute arising from these Clauses will be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

22. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

1. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.
2. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
3. From time to time, the ICO may issue a revised Approved Addendum which:
4. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
5. reflects changes to UK Data Protection Laws;
6. The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.
7. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:
8. its direct costs of performing its obligations under the Addendum; and/or
9. its risk under the Addendum,
10. and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.
11. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

EXHIBIT D
ARTIFICIAL INTELLIGENCE ADDENDUM

Klarity uses cutting edge artificial intelligence software in its products, including large language models (LLMs) that generate text in response to text prompts. To the extent that Klarity uses any artificial intelligence system, algorithm or other software ("**AI**") within its Services, the requirements herein will apply. The definition of AI and requirements herein will apply whether the AI is proprietary to Klarity or a tool made available by a Third Party AI Provider (as defined below).

1. Definitions. As used in this AI Addendum, the following definitions will apply:

   a. "**Third Party AI Provider**" means any third party that uses AI to process Customer Data on Klarity's behalf or provides Klarity with AI that Klarity uses to process Customer Data.

   b. "**Customer Data**" means any information provided by Customer to Klarity to enable the provision of the Services, including information contained in any Customer document processed via the Services.

   c. "**Insulated Information**" means any information that identifies or could be used to identify (i) any individual, household or entity including but not limited to Customer, its Affiliates, employees, contractors, subcontractors, partners or agents; (ii) any Users; or (iii) any prices, products, or services.

2. Model Training. Klarity and Third Party AI Providers will not process any Customer Data for any purpose other than those expressly contemplated within this Agreement. For the avoidance of doubt, Klarity and Third Party AI Providers will not collect, use or retain any Customer Data to train or retrain any global AI model, whether directly or indirectly.

3. Flow Down Requirements. Klarity warrants that, to the extent Klarity engages any Third Party AI Providers to process Customer Data, it will into agreements with all such service providers, which will, at a minimum, be inclusive of obligations and protections for Customer pertaining to confidentiality, privacy, security and data ownership at least as restrictive as those outlined in the Agreement or any of its exhibits. Notwithstanding the foregoing, Klarity will remain liable to Customer for the acts and omissions of Third Party AI Providers to the same extent that Klarity would be liable if Klarity was processing the Customer Data directly.

4. Customer Data. Customer warrants that Customer has the right to provide Customer Data to Klarity and that Customer Data will not infringe upon or otherwise violate any third party intellectual property rights or applicable law.

5. Testing. Klarity may use Customer Data for general product improvement testing, provided that such Customer Data will not contain Insulated Information ("**Global Testing**"). Klarity will perform Global Testing only to improve Klarity's products and services and for no other purpose whatsoever.

6. Deletion. Upon written request by Customer, Klarity will securely and permanently delete any Customer Data unless otherwise required by applicable law.

7. Indemnity. Subject to the terms of the Agreement, Klarity will indemnify, hold harmless, and at Customer's request, defend Customer and its employees, representatives, agents and officers, against all third party claims, liabilities, damages, losses and expenses, including regulatory fines and reasonable attorneys' fees arising from or relating to any violations of the confidentiality, data ownership, privacy and security requirements included herein. Notwithstanding the foregoing, Klarity will not be liable to Customer for third party claims arising out of Customer's use of the Services in a manner inconsistent with Klarity's documented use guidelines or in breach of this Agreement.