TERMS OF SERVICE

These Terms of Service (the “Terms”) govern access to and use of the Klarity Intelligence, Inc. (“Klarity”) website, applications, application connectors, professional services and other services provided by Klarity (the “Services”). All individuals and entities that use the Services and/or create an account with Klarity to use the Services are each individually referred to as “Customer”.

### DEFINITIONS

#### “Affiliate” means any present or future entity controlled by, or under common control with a party.

#### “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.

### ACCEPTANCE OF TERMS

#### By using the Services, you as a Customer accept and agree to follow and be bound by these Terms (whether on behalf of yourself or a legal entity you represent). You also agree to comply with all applicable laws and regulations, as well as all rules or restrictions that are posted on the Services. If you do not agree to these Terms, you are not authorized to use the Services and must cease using the Services without undue delay.

### SERVICES AND SUPPORT

#### Subject to these Terms and any applicable Order Forms, Klarity will use reasonable efforts to provide Customer the Services in accordance with the Service Level Terms and reasonable technical support services (Exhibit A) and Data Processing Addendum (Exhibit B). 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.

#### Customer may order Services from Klarity by entering into a service order in a mutually agreed upon form (an “Order Form”). Each Order Form shall specify, at a minimum, the type and quantities of Service(s), the applicable fees and Subscription Term. Upon execution by both parties, each Order Form shall become effective and be deemed part of these Terms. Klarity shall provide the Services specified in the applicable Order Form during the term specified therein (the “Subscription Term”).

### RESTRICTIONS AND RESPONSIBILITIES

#### 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 (“Software”); modify, translate, or create derivative works based on the Services or any Software (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 or any Software for timesharing or service bureau purposes or otherwise for the benefit of a third; or remove any proprietary notices or labels.

#### Customer represents, covenants, and warrants that Customer and Users will use the Services only in compliance with all applicable laws and regulations and these Terms. 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 these Terms by any User, Customer will promptly notify Klarity.

#### Customer shall be responsible for obtaining and maintaining any equipment and ancillary services needed to connect to, access or otherwise use the Services, including, without limitation, modems, hardware, servers, software, operating systems, networking, web servers and the like (collectively, “Equipment”). Customer shall 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.

#### Klarity will have the right to audit Customer’s use of the Services to verify compliance with these Terms. Klarity may also use the Services to perform such monitoring and enforce the restrictions on Customer’s use of the Services herein.

### CONFIDENTIALITY; PROPRIETARY RIGHTS

#### 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 “Proprietary Information” of the Disclosing Party). Proprietary Information of Klarity includes non-public information regarding features, functionality and performance of the Service. Proprietary Information of Customer includes non-public data provided by Customer to Klarity to enable the provision of the Services, including, but not limited to, terms of each contract, and other potential Customer contracts processed via the Services as agreed in a separate statement of work (collectively, “Customer Agreement”), the parties to each Customer Agreement, and subjects of each Customer Agreement (“Customer Data”). The Receiving Party agrees: (i) to take reasonable precautions to protect such Proprietary 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 Proprietary Information. The Disclosing Party agrees that the foregoing shall not apply with respect to any information after five (5) years following the disclosure thereof or any information that the Receiving Party (a) is or becomes publicly available without breach of these Terms 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 the use of, or reference to, any Confidential Information (e) is required to be disclosed by law, in which case the Receiving Party will provide prompt prior notice to the Disclosing Party.

#### Klarity shall own and retain all right, title and interest in and to (a) the Services and Software, all improvements, enhancements or modifications thereto, (b) any software, applications, inventions or other technology developed in connection with the Services, Software and support, (c) any suggestions, enhancement requests, recommendations or other feedback provided by Customer, including Users, relating to the Services; (d) all intellectual property rights related to any of the foregoing, and (e) all machine learning models derived from Customer Data, provided that all such models shall be trained exclusively on anonymized Customer Data. No rights are granted to Customer hereunder other than as expressly set forth herein.

#### Notwithstanding anything to the contrary, Klarity shall have the right to collect and analyze data and other information relating to the provision, use and performance of various aspects of the Services and related systems and technologies (including, without limitation, information concerning Customer Data and data derived therefrom), and Klarity will be free (during and after the term hereof) to (i) use such information and 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 (ii) disclose such data solely in aggregate or other anonymized, unidentifiable form in connection with its business.

### PAYMENT OF FEES

#### Customer will pay Klarity the then applicable fees described in the Order Form for the Services in accordance with the terms therein (the “Fees”). Unless otherwise provided in an Order Form, all Fees are quoted and payable in United States dollars. The 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).

#### 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.

### TERM AND TERMINATION

#### Subject to earlier termination as provided below, these Terms are 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.

#### Either party may terminate these Terms if the other party (i) breaches any terms and conditions of these Terms 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 these Terms for breach, Klarity agrees to promptly refund to Customer any pre-paid fees, pro-rated for the remainder of the term of these Terms.

#### All sections of these Terms 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.

### WARRANTY AND DISCLAIMER

#### Each party represents and warrants to the other that it has the full authority and power to enter into and perform its obligations under these Terms, and that the execution and performance of these Terms does 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.

#### Klarity further represents and warrants to Customer that the Software will operate substantially in accordance with its documentation. Klarity shall use reasonable efforts consistent with prevailing industry standards to maintain the Services in a manner which minimizes errors and interruptions in the Services and shall perform the 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 shall 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, the 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 shall 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 these Terms will be as provided in the “Term and Termination” section of these Terms. 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 KLARITY DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.

### LIMITATION OF LIABILITY

NOTWITHSTANDING ANYTHING TO THE CONTRARY, EXCEPT FOR BODILY INJURY OF A PERSON, NEITHER PARTY NOR ITS SUPPLIERS (INCLUDING BUT NOT LIMITED TO ALL EQUIPMENT AND TECHNOLOGY SUPPLIERS), OFFICERS, AFFILIATES, REPRESENTATIVES, CONTRACTORS AND EMPLOYEES SHALL BE RESPONSIBLE OR LIABLE WITH RESPECT TO ANY SUBJECT MATTER OF THESE TERMS OR OTHER TERMS AND CONDITIONS RELATED THERETO 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 THESE TERMS 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 SHALL APPLY WITH RESPECT TO ANY CLAIMS BASED ON KLARITY’S BREACH OF CONFIDENTIALITY, DATA PRIVACY OBLIGATIONS, INDEMNITIES OR ON KLARITY’S FRAUD, GROSS NEGLIGENCE OR WILLFUL MISCONDUCT.

### INDEMNIFICATION

#### Klarity shall 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 Software, Services or other materials provided by Klarity, or the use thereof as permitted by these Terms, infringes or otherwise violates any intellectual property rights or applicable law. Klarity has the right to control the defense or settlement of the claim; provided, however, that Klarity may not settle any claim if it imposes any liability or obligation on Customer or its Affiliates without Customer’s prior written consent.

#### Customer shall 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 these Terms infringes or otherwise violates any intellectual property rights or applicable law. Customer has the right to control the defense or settlement of the claim; provided, however, that Customer may not settle any claim if it imposes any liability or obligation on Klarity or its Affiliates without Klarity’s prior written consent.

#### The indemnified party will give the indemnifying party prompt written notice of any claim. 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.

### PUBLICITY

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.

### MISCELLANEOUS

#### Neither party may assign these Terms without the other party’s prior written consent, which consent will not be unreasonably withheld or delayed; provided, however, that a Party may assign these Terms to (a) 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. Subject to the foregoing, these Terms will bind and inure to the benefit of the parties, their respective successors and permitted assigns.

#### All notices under these Terms 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 facsimile or e-mail; 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.

#### If any provision of these Terms is found to be unenforceable or invalid, that provision will be limited or eliminated to the minimum extent necessary so that these Terms will otherwise remain in full force and effect and enforceable. These Terms are 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 these Terms. 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 these Terms 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 these Terms, and all such terms or conditions will be null and void.

#### The parties are independent contractors. No agency, partnership, joint venture, fiduciary or employment is created as a result of these Terms and Customer does not have any authority of any kind to bind Klarity in any respect whatsoever. In any action or proceeding relating to these Terms, the prevailing party will be entitled to recover costs and attorneys’ fees.

#### These Terms shall be governed by the laws of California without regard to its conflict of law provisions. All disputes and legal proceedings related to these Terms will be maintained in courts located in California and the parties consent to the personal jurisdiction of such courts. To the extent permitted by applicable law, each party also hereby waives any right to jury trial in connection with any action or litigation in any way arising out of or related to these Terms.

#### These Terms may be executed by facsimile and in counterparts, which taken together will form one legal instrument.

|  |  |
| --- | --- |
| **Klarity Intelligence, Inc.** | **[CUSTOMER]** |
| By:  | By:  |
| Name:  | Name:  |
| Title:  | Title:  |
|  | Date: June 14, 2022 (“**Effective Date**”) |

Exhibit A

SERVICE LEVEL AGREEMENT

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

1. Customer Support. Klarity will provide Technical Support to Customer via both telephone and e-mail on weekdays during the hours of 8:00 am through 5:00 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 Terms.
2. System Uptime Availability. During the Subscription Term, the Klarity Platform and any other purchased modules, including Klarity RevRec, Klarity Billing and Klarity Legal (“**Klarity Services**”) shall be available 99.7% (“**Target Availability Percentage**”), measured monthly, excluding holidays and 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 or downtime 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. Failure to provide such written notice will forfeit the right to receive Service Credit (as defined below). Klarity will provide Customer with a credit for any verified Downtime (the “Service Credit”) as follows:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Availability (%) | 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 |

1. Service Credit Terms. 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 and exclusive 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”) applies to Klarity Intelligence, Inc. (“Klarity”) Processing of Personal Data provided to Klarity by Customer as part of Klarity’s provision of Services to Customer. This DPA forms a part of and is subject to the Terms between Klarity and Customer to reflect the parties’ agreement with regard to the Processing of Personal Data.

In the course of providing Services to Customer pursuant to this DPA, Klarity may Process Personal Data on behalf of Customer and the parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

The terms of this DPA will be effective and replace any previously applicable data processing terms as of the date of last signature.

Introduction

1. Customer is a Controller of certain Personal Data and wishes to appoint Klarity as a Processor to Process this Personal Data on its behalf.
2. The parties are entering into this DPA to ensure that Klarity conducts such data Processing in accordance with Customer's instructions and Applicable Data Protection Law requirements, and with full respect for the fundamental data protection rights of the Data Subjects whose Personal Data will be Processed.

Definitions

In this DPA, the following terms shall have the following meanings:

“Business,” “Business Purpose,” “Consumer,” “Person,” “Personal Information,” “Sell,” “Service Provider,” and “Third Party” shall have the meanings set forth in the CCPA.

“CCPA” means the California Consumer Privacy Act of 2018 and its implementing regulations.

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

“Customer Personal Information” means any Data maintained by Customer and processed by Klarity solely on Customer’s behalf, that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household, to the extent that such information is protected as “personal information” (or an analogous variation of such term) under applicable U.S. Data Protection Law.

"Applicable Data Protection Law" shall 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) the CCPA, (iv) any national legislation made under or pursuant to (i), (ii), (iii) or (iv); and (v) any amendments or successor legislation to (i), (ii), (iii), (iv), or (v); and any other applicable data protection law.

"Privacy Shield" means the EU-US Privacy Shield self-certification program operated by the U.S. Department of Commerce and approved by the European Commission pursuant to Decision C(2016)4176 of July 12, 2016.

“U.S. Data Protection Law” means all laws and regulations of the United States of America, including the CCPA, applicable to the processing of “personal information” (or an analogous variation of such term).

Data Protection

Relationship of the parties. Customer (the Controller) appoints Klarity as a Processor to Process the Personal Data that is the subject matter of the Terms (the "Data"). Each party shall comply with the obligations that apply to it under Applicable Data Protection Law.

Purpose limitation. Klarity shall Process the Data as a Processor only as necessary to perform its obligations under the Terms, and strictly in accordance with the documented instructions of Customer (the "Permitted Purpose"), except where otherwise required by any EU (or any EU Member State) law applicable to Klarity. In no event shall Klarity Process the Data for its own purposes or those of any third party except as set forth in the Terms.

International transfers. Klarity shall 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 as Exhibit C.

Confidentiality of Processing. Klarity shall ensure that any person that it authorizes to Process the Data (including Klarity's staff, agents and subcontractors) (an "Authorized Person") shall be subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty) and shall not permit any person to Process the Data who is not under such a duty of confidentiality. Klarity shall ensure that all Authorized Persons Process the Data only as necessary for the Permitted Purpose.

Security. Klarity shall 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 Data or the physical, technical, administrative, or organizational safeguards put into place by Klarity (a "Security Incident"). Such measures shall 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 creation, collection, receipt, access, use, storage, disposal, and disclosure of Personal Information does and will comply with all Applicable Data Protection Law. Klarity shall 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:

A. the anonymization and encryption of Personal Data;

B. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;

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

D. a Process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

Subprocessing. Customer specifically authorizes the engagement of Klarity’s affiliates as subprocessors. Klarity Customer consents to Klarity engaging third party subprocessors to Process the Data provided that: (i) Klarity notifies Customer in writing (email sufficient) prior to such subprocessor processing any Personal Information, (ii) Klarity imposes data protection terms on any subprocessor it appoints that protect the Data to 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 or replacement of a third party subprocessor 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. Customer specifically consents to Klarity using the following subprocessors:

|  |  |
| --- | --- |
| Subprocessor | Description of Processing |
| Amazon Web Services, Inc. (AWS) | Klarity’s infrastructure is entirely hosted on AWS. |
| MongoDB, Inc. | Klarity uses MongoDB’s database hosted on AWS for persistent 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 request. Klarity does not store any contracts or other documents containing personal data in Asana. |
| Google LLC | Klarity uses Google to communicate with Customer and to send and receive Customer’s documents.  |
| Slack Technologies, LLC | Klarity uses Slack for Customer support engagement.  |
| 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). The data stored in Elastic Cloud will be limited to document and user attributes, such as User IDs, Governing Law distribution and Termination period day counts. Elastic Cloud is currently in use by multiple Fortune 500 companies and Governments.  |
| Khosla Labs Pvt. Ltd. | Khosla Labs is Klarity’s long-term Klarity of implementation/annotation services headquartered in Bangalore, India. Klarity has had a long-term contract with Khosla Labs since 2017. |

Cooperation and Data Subjects' rights. Klarity shall 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 shall promptly inform Customer providing details of the same.

Data Protection Impact Assessment. If Klarity believes or becomes aware that its Processing of the Data is likely to result in a high risk to the data protection rights and freedoms of Data Subjects, it shall promptly inform Customer and provide Customer with all such reasonable and timely assistance as Customer may require in order to conduct a data protection impact assessment and, if necessary, consult with its relevant data protection authority.

Security incidents. Upon becoming aware of a Security Incident, Klarity shall inform Customer within 48 hours and shall provide all such timely information and cooperation as Customer may require in order for Customer to fulfil its data breach reporting obligations under (and in accordance with the timescales required by) Applicable Data Protection Law. Klarity shall further at its own expense take all such measures and actions as are necessary to remedy or mitigate the effects of the Security Incident and shall keep Customer apprised of all developments in connection with the Security Incident. Klarity agrees that it shall 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 Customer shall 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.

Deletion or return of Data. After termination or expiry of the Terms, or upon Customer’s request, Klarity shall destroy or return to Customer (at Customer’s option) all Data (including all copies of the Data) in its possession or control (including any Data subcontracted to a third party for Processing). This requirement shall not apply to the extent that Klarity is required by any EU (or any EU Member State) law to retain some or all of the Data, in which event Klarity shall isolate and protect the Data from any further Processing except to the extent required by such law.

CCPA Compliance. As between the parties, Customer is a Business and appoints Klarity as a Service Provider to process Customer Personal Information on behalf of Customer. 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. Klarity certifies that it understands the foregoing restriction and will comply with it in accordance with applicable U.S. Data Protection Law. All matters arising out of or relating to this DPA concerning rights or obligations under the CCPA shall be interpreted and construed in accordance with the law of the State of California. Any legal action or proceeding arising out of or relating to this DPA concerning rights or obligations under the CCPA shall be brought exclusively in the U.S. District Court for the Northern District of California (unless that court does not have jurisdiction over the action or proceeding, in which case the action or proceeding shall be brought exclusively in state court in San Francisco, California).

Audit. Klarity shall 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 shall 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; or (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.

Indemnification. Klarity shall defend, indemnify, and hold harmless Customer, and its subsidiaries, affiliates, and their respective officers, directors, employees, agents, successors, and permitted assigns (each, a "Customer Indemnitee") from and against all losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, penalties, fines, costs, or expenses of whatever kind, including reasonable attorneys' fees, the cost of enforcing any right to indemnification hereunder, and the cost of pursuing any insurance providers, arising out of or resulting from any third-party claim against any Customer Indemnitee directly arising out of or resulting from Klarity's failure to comply with any of its obligations under this DPA. Any limitation of liability in the Terms shall not apply to Klarity’s Indemnification obligations under this section.

Mandatory Disclosure. Klarity acknowledges that Customer may disclose this DPA and any relevant privacy provisions in the Terms to the US Department of Commerce, the Federal Trade Commission, European data protection authority, or any other US or EU judicial or regulatory body upon their request and that any such disclosure shall not be deemed a breach of the Terms or this DPA. Notwithstanding any provision of the Terms or this DPA, 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.

Choice of Law. All matters arising out of or relating to this DPA shall be interpreted and construed in accordance with the laws of Ireland, without regard to the conflict of laws provisions thereof to the extent such provisions would require or permit the application of laws of any jurisdiction other than those of the State of California. The United Nations Convention on the International Sale of Goods will not apply to this DPA. Any legal action or proceeding arising out of or relating to this DPA shall be brought exclusively in Ireland, and each party irrevocably submits to the sole and exclusive jurisdiction of these courts in any action or proceeding. The parties waive their right to a jury trial in any action or proceeding arising out of or related to this DPA.

EXHIBIT C

**Standard Contractual Clauses for the Transfer of Personal Data**

Customer, as specified in the Terms 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]](#endnote-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 shall have the same meaning as in that Regulation.

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

(c) These Clauses shall 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 shall 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 – Optional***

**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 shall 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 shall 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 shall 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 shall immediately inform the data exporter if it is unable to follow those instructions.

**8.2   Purpose limitation**

The data importer shall 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 shall 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 shall 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 shall 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 shall inform the data exporter without undue delay. In this case, the data importer shall 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 shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, 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 shall 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 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 shall 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 shall 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 shall 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 shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall 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 shall 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 shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall 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 shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall 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 shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

**8.8   Onward transfers**

The data importer shall 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]](#endnote-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.

**8.9   Documentation and compliance**

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

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

(c) The data importer shall 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 shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall 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) OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter’s prior specific written authorisation. The data importer shall submit the request for specific authorisation at least [*Specify time period*] prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter’s general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [*Specify time period*] 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 shall 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 shall 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]](#endnote-3)) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall 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 shall 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 shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

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

(b) The data importer shall 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 shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall 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 shall comply with the instructions from the data exporter.

***Clause 11***

**Redress**

(a) The data importer shall 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 shall deal promptly with any complaints it receives from a data subject.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body ([[4]](#endnote-4)) at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

 (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall 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 shall 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 shall 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 shall 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 shall be liable to the data subject, and the data subject shall 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 shall be liable to the data subject, and the data subject shall 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 shall 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 shall 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 shall 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**

1. [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, shall 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, shall 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, shall 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 shall 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 ([[5]](#endnote-5));

(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 shall 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 shall 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 shall 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) shall 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:

(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 shall 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 shall 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 shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall 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 shall 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 shall 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 shall 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 shall 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 shall 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) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall 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**

[OPTION 1: These Clauses shall 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 shall be the law of \_\_\_\_\_\_\_ (*specify Member State*).]

[OPTION 2: These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of \_\_\_\_\_\_\_ (*specify Member State*).]

***Clause 18***

**Choice of forum and jurisdiction**

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of  \_\_\_\_\_ (*specify Member State*).

(c) 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.

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

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](https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=OJ:L:2018:295:TOC)), 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. [↑](#endnote-ref-1)
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. [↑](#endnote-ref-2)
3. This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7. [↑](#endnote-ref-3)
4. The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards. [↑](#endnote-ref-4)
5. 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.

ANNEX 1 to the Standard Contractual Clauses

**PARTIES AND DETAILS OF PROCESSING**

**A. LIST OF PARTIES**

**Data exporter**

The data exporter is the Customer or its employees or affiliates.

**Name:** Customer as specified in the Terms

**Address:**

**Contact person’s name, position and contact details:**

**Activities relevant to the data transferred under these Clauses:** as per the Terms, 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. (as defined in the DPA).

**Name:** Klarity Intelligence, Inc.

**Address:** 244 Kearny Street, 5th Floor, San Francisco, CA 94108

**Contact person’s name, position and contact details: Grant Oglesby, Corporate Counsel,** **grant@klaritylaw.com****, (408) 691-9625**

**Activities relevant to the data transferred under these Clauses:** as per the Terms, 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)
	* Klarity, Position
	* Login Credentials**Special categories of data (if appropriate)**

The personal data transferred concerns the following special categories:

**Processing operations**

The personal data transferred will be subject to the following basic processing activities:

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 Terms in accordance with the terms of the DPA.

**Nature of the processing**

Klarity will provide, secure and monitor the Services in accordance with the Terms. Klarity receives, stores, structures, categorizes, analyzes, handles, processes and sends Personal Data on behalf of Customer in accordance with the Terms. Klarity shall Process the Data only as necessary to perform its obligations under the Terms.

**Purpose(s) of the data transfer and further processing**

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

**The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period**

For the duration of the Terms until deletion in accordance with the provisions of the DPA. After termination or expiry of the Terms, or upon Customer’s request, Klarity shall destroy or return to Customer (at Customer’s option) all Data (including all copies of the Data) in its possession or control (including any Data subcontracted to a third party for Processing). This requirement shall not apply to the extent that Klarity is required by any EU (or any EU Member State) law to retain some or all of the Data, in which event Klarity shall isolate and protect the Data from any further Processing except to the extent required by such law.

**For transfers to (sub-)processors, also specify subject matter, nature and duration of the processing**

Subject matter, nature and duration of the processing for transfers to (sub-)processors is described in Section 6 of 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 INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

**Measures of pseudonymisation and encryption of personal data**

Klarity shall 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 anonymization and encryption of Personal Data. Klarity maintains Personal 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 shall 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 ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services. Klarity shall 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 Data or the physical, technical, administrative, or organizational safeguards put into place by Klarity (a "Security Incident"). Such measures shall 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 represents and warrants that its creation, collection, receipt, access, use, storage, disposal, and disclosure of Personal Information does and will comply with all Applicable Data Protection Law. All employees are required to undergo information security and privacy training. Klarity shall 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 Personal Data; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services; (iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (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 shall 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 Personal Data in a timely manner in the event of a physical or technical incident. Klarity performs regular backups of Personal Data, which is hosted in AWS data centers. Backups are retained redundantly across multiple availability zones and encrypted in transit (HTTPS/TLS) and at rest (AES-256).

**Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing**

Klarity shall 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 Personal 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 shall ensure that any person that it authorizes to Process the Data including Klarity's Authorized Persons shall be subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty) and shall not permit any person to Process the Data who is not under such a duty of confidentiality. Klarity shall ensure that all Authorized Persons Process the Data only as necessary for the Permitted Purpose. Klarity shall 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 as Exhibit C.

**Measures for the protection of data during storage**

Personal Data is stored encrypted using AES-256.

**Measures for ensuring physical security of locations at which personal data are processed**

Klarity provides access to the facilities to those employees and contractors who have a legitimate business need for such access privileges. The Services operate on Amazon Web Services (“AWS”) and are protected by the security and environmental controls of Amazon.

**Measures for ensuring events logging**

Klarity monitors access to applications, tools, and resources that process or store Customer 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**

Bi-annual 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; and passwords must include at least one uppercase letter, one lowercase letter and one number. Passwords and IT system credentials are stored only on Bitwarden, Klarity’s self-hosted password management system. Passwords are not communicated over anything other than snappass.klaritylaw.com (an internal, non-internet facing system that wipes passwords immediately after they are viewed). 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 2 Type II and SOC 1 Type I 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**

After termination or expiry of the Terms, or upon Customer’s request, Klarity shall destroy or return to Customer (at Customer’s option) all Data (including all copies of the Data) in its possession or control (including any Data subcontracted to a third party for Processing). This requirement shall not apply to the extent that Klarity is required by any EU (or any EU Member State) law to retain some or all of the Data, in which event Klarity shall 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 platform), Avast Pro Plus (Antivirus) and Rippling (MDM). All infosec policies detail consequences for violation and the CTO takes responsibility for enforcing these.

**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 specifically authorizes the engagement of Klarity’s affiliates as subprocessors. Customer consents to Klarity engaging third party subprocessors to Process the Data provided that: (i) Klarity notifies Customer in writing (email sufficient) prior to such subprocessor processing any Personal Information, (ii) Klarity imposes data protection terms on any subprocessor it appoints that protect the Data to substantially similar terms to the terms of the DPA; and (iii) Klarity remains fully liable for any breach of the DPA that is caused by an act, error or omission of its subprocessor. Customer may object to Klarity's appointment or replacement of a third party subprocessor 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 the DPA.

**ANNEX 3 to the Standard Contractual Clauses**

**LIST OF SUB-PROCESSORS**

Customer specifically consents to Klarity using subprocessors as forth in the Section 6 of the DPA.

**Sub-processors that are currently engaged by Klarity:**

|  |  |  |  |
| --- | --- | --- | --- |
| ***Name*** | ***Address*** | ***Contact person’s name, position and contact details*** | ***Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised)*** |
| Amazon Web Services, Inc. (AWS) | 410 Terry Avenue North, Seattle WA 98109-5210USA | Stephen Schmidt, Vice President, Security Engineering & Chief Information Security Officer | Klarity’s infrastructure is entirely hosted on AWS. |
| MongoDB, Inc. | 1633 Broadway 38th Floor New York NY 10019USA | Rachael McClure, Legal Director at MongoDB | Klarity uses MongoDB’s database hosted on AWS for persistent storage of data points extracted from contracts. |
| Asana, Inc. | 1550 Bryant Street Suite 200 San FranciscoCA 94103 USA | Eleanor Lacey, General Counsel and Corporate Secretary | Klarity uses Asana to track customer feature requests and bug reports that often include personal data of customer’s employees who submitted such request. Klarity does not store any contracts or other documents containing personal data in Asana. |
| Google LLC | 1600 Amphitheatre Parkway Mountain View CA 94043USA | Emil Ochotta, Principal Software Engineer, DPO, and Lead of Privacy Governance https://support.google.com/cloud/contact/dpo | Klarity uses Google to communicate with Customer and to send and receive Customer’s documents.  |
| Slack Technologies, LLC | 500 Howard StreetSan Francisco, CA 94105 USA | Megan Cristina, Chief Privacy Officer, dpo@slack.com | Klarity uses Slack for Customer support.  |
| Elasticsearch, B.V. | 800 W El Camino Real Ste. 350Mountain ViewCA 94040 USA | W.H. Baird Garrett, SVP of Legal, General Counsel and Secretary | For customers who choose to use our optional analytics module, Klarity Analytics will be hosted on Elastic Cloud (using AWS for underlying storage). The data stored in Elastic Cloud will be limited to document and user attributes, such as User IDs, Governing Law distribution and Termination period day counts.  |
| Khosla Labs Pvt. Ltd. | Second Floor, GRS Tower, #18/2A, Marathahalli - Sarjapur Rd, Above Café Coffee Day, Bengaluru, Karnataka 560103, India | Vasanth Babu, HR & Admin Lead, babu@khoslalabs.com | 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. |

**ANNEX 4 to the Standard Contractual Clauses**

**2021 EU STANDARD CONTRACTUAL CLAUSES - CONTROLLER TO PROCESSOR**

Where applicable pursuant to the DPA, the parties hereby enter into the Module Two (Controller to Processor) of Standard Contractual Clauses. These Standard Contractual Clauses apply with respect to the transfer of personal data as specified in Annex 1. Klarity agrees that it shall abide by: (i) the terms of the Standard Contractual Clauses Sections I, II, III and IV (as applicable) as set out in Exhibit C, in the manner described in Annex 1, 2, 3 and 4 to these Terms. Where the Standard Contractual Clauses (Module Two - Controller to Processor) require the parties to choose between optional clauses, the parties have done so as set out below:

	* 1. The Optional Clause 7 “Docking clause” shall be adopted.
		2. For Clause 9 “Use of sub-processors”, the parties elect the following option:*“(a) OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter’s general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least* ***ten (10) calendar 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 shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.”*

	* 1. For Clause 11 (a) “Redress”, the parties do not adopt the option.
		2. For Clause 17 “Governing law”, the parties elect the following option:*“Option 1. These Clauses shall 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 shall be the law of* ***Ireland****.”*

	* 1. For Clause 18 (b) “Choice of Forum and Jurisdiction”:*“The Parties agree that those shall be the courts of* ***Ireland****”.* [↑](#endnote-ref-5)