DATA PROCESSING ADDENDUM

Last Updated: May 1, 2022.

This Data Processing Addendum ("DPA") forms part of the Subscription Agreement available at https://drata.com/terms (collectively, the "Agreement") between the parties under which Drata will provide certain services (collectively, the "Services") to Customer. This DPA consists of the main body and Schedules 1, 2, 3, and 4. To complete this DPA, the Parties must sign and date in the provided signature region of the main body of this DPA and Schedules 1 and 2. Execution of this DPA by Customer shall be deemed to constitute signature and acceptance by Customer of the Standard Contractual Clauses (defined hereinafter) and their Appendices, which are incorporated herein by reference herein in their entireties. If the Customer entity signing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement. If the Customer entity signing the DPA is not a party to an Order Form nor an Agreement directly with Drata, but is instead a customer indirectly via an authorized reseller of Drata services, this DPA is not valid and is not legally binding. Such entity should contact the authorized reseller to discuss whether any amendment to its agreement with that reseller may be required.

HOW TO EXECUTE THIS DPA

1. This DPA consists of two parts: the main body of the DPA, and Schedules 1 – 4.

2. This DPA has been pre-signed on behalf of Drata. Schedule 2 has been pre-signed by Drata, Inc. as the data importer.

3. To complete this DPA, Customer must:

   a. Complete the information in the signature box of this DPA and sign this DPA.

   b. Send the signed DPA to Drata by email to legal@drata.com.

Except as otherwise expressly provided in the Agreement, this DPA will become legally binding upon receipt by Drata of the validly completed DPA at the above email address. For the avoidance of doubt, signature of this DPA shall be deemed to constitute signature and acceptance of the Standard Contractual Clauses, including Schedule 2. Where Customer wishes to separately execute the Standard Contractual Clauses and its Appendix, Customer should also complete the information as the data exporter and sign Schedule 2.

1. Definitions

   For purposes of this DPA, the terms below have the meanings set forth below. Capitalized terms that are used but not defined in this DPA have the meanings given in the Agreement.

   1.1. Authorized Affiliate means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity, where "control" refers to the power to direct or cause the direction of the subject entity, whether through ownership of voting securities, by contract or otherwise.

   1.2. Applicable Data Protection Laws means the privacy, data protection and data security laws and regulations of any jurisdiction applicable to the Processing of Personal Data under the Agreement, including, without limitation, European Data Protection Laws and the CCPA.

1.3. CCPA means the California Consumer Privacy Act of 2018 and any regulations promulgated thereunder, in each case, as amended from time to time, including the California Privacy Rights Act of 2020, and any regulations promulgated thereunder.

1.4. EEA means the European Economic Area.

1.5. European Data Protection Laws means the GDPR and other data protection laws and regulations of the European Union, its Member States, Switzerland, Iceland, Liechtenstein, Norway and the United Kingdom, in each case, to the extent applicable to the Processing of Personal Data under the Agreement.

1.6. GDPR means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, as amended from time to time.

1.7. Information Security Incident means a breach of Drata's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data in Drata's possession, custody or control. Information Security Incidents do not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems.

1.8. Personal Data means Customer Content that constitutes "personal data," "personal information," or "personally identifiable information" defined in Applicable Data Protection Laws, or information of a similar character regulated thereby, except that Personal Data does not include such information pertaining to Customer's personnel or representatives who are business contacts of Drata, where Drata acts as a controller of such information.

1.9. Processing means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.10. Security Measures has the meaning given in Section 4(a) (Drata's Security Measures).

1.11. Standard Contractual Clauses means Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as currently set out at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

1.12. Subprocessors means third parties that Drata engages to Process Personal Data in relation to the Services.

1.13. The terms controller, data subject, processor and supervisory authority as used in this DPA have the meanings given in the GDPR.

2. Duration and Scope of DPA

2.1. This DPA will remain in effect so long as Drata Processes Personal Data, notwithstanding the expiration or termination of the Agreement.

2.2. Schedules 1 and 2 to this DPA apply solely to Processing subject to European Data Protection Laws. Schedule 3 to this DPA applies solely to Processing subject to the CCPA to the extent Customer is a "business" (as defined in CCPA) with respect to such Processing.

3. Customer Instructions

Drata will Process Personal Data only in accordance with Customer's instructions to Drata. This DPA is a complete expression of such instructions, and Customer's additional instructions will be binding on Drata only pursuant to an amendment to this DPA signed by both parties. Customer instructs Drata to Process Personal Data to provide the Services and as authorized by the Agreement.

4. Security

4.1. Drata Security Measures. Drata will implement and maintain administrative, technical and physical safeguards designed to protect the security and integrity of Personal Data, prevent Information Security Incidents (the "Security Measures"). The Security Measures shall at a minimum include the measures described in Schedule 4 and any other measures required by Applicable Data Protection Laws. Drata may update the Security Measures from time to time, so long as the updated measures do not materially decrease the overall protection of Personal Data.

4.2. Information Security Incidents. Drata will notify Customer without undue delay of any Information Security Incident of which Drata becomes aware. Such notifications will describe available details of the Information Security Incident, including steps taken to mitigate the potential risks and steps Drata recommends the Customer take to address the Information Security Incident. Drata's notification of or response to an Information Security Incident will not be construed as Drata's acknowledgement of any fault or liability with respect to the Information Security Incident.

4.3. Reviews and Audits of Compliance

4.4. Customer may audit Drata's compliance with its obligations under this DPA up to once per year and on such other occasions as may be required by European Data Protection Laws, including if mandated by Customer's supervisory authority. Drata will contribute to such audits by providing Customer or Customer's supervisory authority with the information and assistance reasonably necessary to conduct the audit. If a third party is to conduct the audit, Drata may object to the auditor if the auditor is, in Drata's reasonable opinion, not independent, a competitor of Drata, or otherwise manifestly unsuitable. Such objection by Drata will require the Customer to appoint another auditor or conduct the audit itself. To request an audit, Customer must submit a proposed audit plan to Drata at least two weeks in advance of the proposed audit date and any third-party auditor must sign a customary non-disclosure agreement mutually acceptable to the parties (such acceptance not to be unreasonably withheld) providing for the confidential treatment of all information exchanged in connection with the audit and any reports regarding the results or findings thereof. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. Drata will review the proposed audit plan and provide Customer with any concerns or questions (for example, any request for information that could compromise Drata security, privacy, employment or other relevant policies). Drata will work cooperatively with Customer to agree on a final audit plan. Nothing in this Section 2(b) shall require Drata to breach any duties of confidentiality. If the controls or measures to be assessed in the requested audit are addressed in an SOC 2 Type 2, ISO, NIST or similar audit report performed by a qualified third party auditor within twelve (12) months of Customer's audit request and Drata has confirmed there have been no known material changes in the controls audited since the date of such report, Customer agrees to accept such report in lieu of requesting an audit of such controls or measures. The audit must be conducted during regular business hours, subject to the agreed final audit plan and Drata's safety, security or other relevant policies, and may not unreasonably interfere with Drata business activities. Customer will promptly notify Drata of any non-compliance discovered during the course of an audit and provide Drata any audit reports generated in connection with any audit under this Section 2(b), unless prohibited by European Data Protection Laws or otherwise instructed by a supervisory authority. Customer may use the audit reports only for the purposes of meeting Customer's regulatory audit requirements and/or confirming compliance with the requirements of this DPA. Any audits are at Customer's sole expense. Customer shall reimburse Drata for any time expended by Drata and any third parties in connection with any audits or inspections under this Section 2(b) at Drata's then-current professional services rates, which shall be made

available to Customer upon request. Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit.

4.5. Impact Assessments and Consultations

4.6. Drata will (taking into account the nature of the Processing and the information available to Drata) reasonably assist Customer in complying with its obligations under Articles 35 and 36 of the GDPR, by (a) making available documentation describing relevant aspects of Drata's information security program and the security measures applied in connection therewith and (b) providing the other information contained in the Agreement, including this DPA.

4.7. Customer's Responsibilities

4.7.1. Customer Obligations. Without limitation of Customer's obligations under the Agreement, Customer (a) agrees that Customer is solely responsible for its use of the Services, including (1) making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Personal Data, (2) securing the account authentication credentials, systems and devices Customer uses to access the Services, (3) securing Customer's systems and devices that Drata uses to provide the Services, and (4) backing up Personal Data; (b) shall comply with its obligations under Applicable Data Protection Laws; and (c) shall ensure (and is solely responsible for ensuring) that its instructions in Section 3 comply with Applicable Data Protection Laws, and that Customer has given all notices to, and has obtained all such notices from, individuals to whom Personal Data pertains and all other parties as required by applicable laws or regulations for Drata to Process Personal Data as contemplated by the Agreement. (d) Customer shall comply with its obligations under Applicable Data Protection Laws.

4.7.2. Prohibited Data. Customer represents and warrants to Drata that Customer Data does not and will not, without Drata's prior written consent, contain any social security numbers or other government-issued identification numbers, protected health information subject to the Health Insurance Portability and Accountability Act (HIPAA) or other information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; health insurance information; biometric information; passwords for online accounts; credentials to any financial accounts; tax return data; credit reports or consumer reports; any payment card information subject to the Payment Card Industry Data Security Standard; information subject to the Gramm-Leach-Bliley Act, Fair Credit Reporting Act or the regulations promulgated under either such law; information subject to restrictions under Applicable Data Protection Laws governing Personal Data of children, including, without limitation, all information about children under 16 years of age; or any information that falls within any special categories of data (as defined in GDPR).

5. Data Subject Rights

5.1. Data Subject Request Assistance. Drata will (taking into account the nature of the Processing of Personal Data) provide Customer with assistance reasonably necessary for Customer to perform its obligations under Applicable Data Protection Laws to fulfill requests by data subjects to exercise their rights under Applicable Data Protection Laws ("Data Subject Requests") with respect to Personal Data in Drata's possession or control. Customer shall compensate Drata for any such assistance at Drata's then-current professional services rates, which shall be made available to Customer upon request.

5.2. Customer's Responsibility for Requests. If Drata receives a Data Subject Request, Drata will advise the data subject to submit the request to Customer and Customer will be responsible for responding to the request.

6. Europe Specific Provisions.

6.1. Definitions. For the purposes of this section 12 and Schedule 1 these terms shall be defined as follows:

6.1.1."EU C-to-P Transfer Clauses" means Standard Contractual Clauses sections I, II, III and IV (as applicable) to the extent they reference Module Two (Controller-to-Processor).

6.1.2."EU P-to-P Transfer Clauses" means Standard Contractual Clauses sections I, II III and IV (as applicable) to the extent they reference Module Three (Processor-to-Processor).

6.2. GDPR. Drata will Process Personal Data in accordance with the GDPR requirements directly applicable to Drata's provision of its Services.

6.3. Customer Instructions. Drata shall inform Customer immediately (i) if, in its opinion, an instruction from Customer constitutes a breach of the GDPR and/or (ii) if Drata is unable to follow Customer's instructions for the Processing of Personal Data.

6.4. Transfer mechanisms for data transfers. If, in the performance of the Services, Personal Data that is subject to the GDPR or any other law relating to the protection or privacy of individuals that applies in Europe is transferred out of Europe to countries which do not ensure an adequate level of data protection within the meaning of the European Data Protection Laws, the transfer mechanisms listed below shall apply to such transfers and can be directly enforced by the Parties to the extent such transfers are subject to the European Data Protection Laws:

6.4.1.The EU C-to-P Transfer Clauses. Where Customer and/or its Authorized Affiliate is a Controller and a data exporter of Personal Data and Drata is a Processor and data importer in respect of that Personal Data, then the parties shall comply with the EU C-to-P Transfer Clauses, subject to the additional terms in Schedule 1; and/or

6.4.2.The EU P-to-P Transfer Clauses. Where Customer and/or its Authorized Affiliate is a Processor acting on behalf of a Controller and a data exporter of Personal Data and Drata is a Processor and data importer in respect of that Personal Data, the parties shall comply with the terms of the EU P-to-P Transfer Clauses, subject to the additional terms in Schedule 1.

6.5. Impact of local laws. As of the Effective Date, Drata has no reason to believe that the laws and practices in any third country of destination applicable to its Processing of the Personal Data as set forth in the Infrastructure and Subprocessors Documentation, including any requirements to disclose Personal Data or measures authorizing access by a Public Authority, prevent Drata from fulfilling its obligations under this DPA. If Drata reasonably believes that any existing or future enacted or enforceable laws and practices in the third country of destination applicable to its Processing of the Personal Data ("Local Laws") prevent it from fulfilling its obligations under this DPA, it shall promptly notify Customer. In such a case, Drata shall use reasonable efforts to make available to the affected Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to facilitate compliance with the Local Laws without unreasonably burdening Customer. If Drata is unable to make available such change promptly, Customer may terminate the applicable Order Form(s) and suspend the transfer of Personal Data in respect only to those Services which cannot be provided by Drata in accordance with the Local Laws by providing written notice in accordance with the "Notices" section of the Agreement. Customer shall receive a refund of any prepaid fees for the period following the effective date of termination for such terminated Services.

7. Subprocessors

7.1. Consent to Subprocessor Engagement. Customer specifically authorizes the engagement of Drata's Affiliates as Subprocessors and generally authorizes the engagement of other third parties as Subprocessors ("Subprocessors").

7.2. Information about Subprocessors. Information about Subprocessors, including their functions and locations, is available at: https://drata.com/sub-processors (as may be updated by Drata from time to time) or such other website address as Drata may provide to Customer from time to time (the "Subprocessor Site").

7.3. Requirements for Subprocessor Engagement. When engaging any Subprocessor, Drata will enter into a written contract with such Subprocessor containing data protection obligations not less protective than those in this DPA with respect to Personal Data to the extent applicable to the nature of the services provided by such Subprocessor. Drata shall be liable for all obligations under the Agreement subcontracted to, the Subprocessor or its actions and omissions related thereto.

7.4. Opportunity to Object to Subprocessor Changes. When Drata engages any new Third Party Subprocessor after the effective date of the Agreement, Drata will notify Customer of the engagement (including the name and location of the relevant Subprocessor and the activities it will perform) by updating the Subprocessor Site or by other written means. If Customer objects to such engagement in a written notice to Drata within 15 days after being informed of the engagement on reasonable grounds relating to the protection of Personal Data, Customer and Drata will work together in good faith to find a mutually acceptable resolution to address such objection. If the parties are unable to reach a mutually acceptable resolution within a reasonable timeframe, Customer may, as its sole and exclusive remedy, terminate the Agreement and cancel the Services by providing written notice to Drata and pay Drata for all amounts due and owing under the Agreement as of the date of such termination.

8. Miscellaneous

Except as expressly modified by the DPA, the terms of the Agreement remain in full force and effect. In the event of any conflict or inconsistency between this DPA and the other terms of the Agreement, this DPA will govern. Notwithstanding anything in the Agreement or any order form entered in connection therewith to the contrary, the parties acknowledge and agree that Drata's access to Personal Data does not constitute part of the consideration exchanged by the parties in respect of the Agreement. Notwithstanding anything to the contrary in the Agreement, any notices required or permitted to be given by Drata to Customer under this DPA may be given (a) in accordance with any notice clause of the Agreement; (b) to Drata's primary points of contact with Customer; or (c) to any email provided by Customer for the purpose of providing it with Services-related communications or alerts. Customer is solely responsible for ensuring that such email addresses are valid.

IN WITNESS WHEREOF, the undersigned have executed this Agreement by their duly authorized representatives, with the intention to be legally bound.

CUSTOMER NAME:_____

By:_____

Name:_____

Title:_____

Date:_____

DRATA INC.

By:_____
DocuSigned by:
Adam Markowitz
FE45BCC0E8C1435...

Name: Adam Markowitz

Title: CEO

Date: 5/2/2022

SCHEDULE 1

TRANSFER MECHANISMS FOR EUROPEAN DATA TRANSFERS

For the purposes of the EU C-to-P Transfer Clauses and the EU P-to-P Transfer Clauses, Customer is the data exporter and Drata is the data importer and the parties agree to the following. If and to the extent an Authorized Affiliate relies on the EU C-to-P Transfer Clauses or the EU P-to-P Transfer Clauses for the transfer of Personal Data, any references to 'Customer' in this Schedule include such Authorized Affiliate. Where this Schedule 1 does not explicitly mention EU C-to-P Transfer Clauses or EU P-to-P Transfer Clauses it applies to both of them.

1. **STANDARD CONTRACTUAL CLAUSES OPERATIVE PROVISIONS AND ADDITIONAL TERMS**

1.1. **Reference to the Standard Contractual Clauses**. The relevant provisions contained in the Standard Contractual Clauses are incorporated by reference and are an integral part of this DPA. The information required for the purposes of the Appendix to the Standard Contractual Clauses are set out in Schedule 2.

1.2. **Docking clause**. The option under clause 7 shall not apply.

1.3. **Instructions**. This DPA and the Agreement are Customer's complete and final documented instructions at the time of signature of the Agreement to Drata for the Processing of Personal Data. Any additional or alternate instructions must be consistent with the terms of this DPA and the Agreement. For the purposes of clause 8.1(a), the instructions by Customer to Process Personal Data include onward transfers to a third party located outside Europe for the purpose of the performance of the Services.

1.4. **Certification of Deletion**. The parties agree that the certification of deletion of Personal Data that is described in clause 8.5 and 16(d) of the Standard Contractual Clauses shall be provided by Drata to Customer only upon Customer's written request.

1.5. **Audits of the SCCs**. The parties agree that the audits described in clause 8.9 of the Standard Contractual Clauses shall be carried out in accordance with section 4.3 of this DPA.

1.6. **General authorization for use of Subprocessors**. Option 2 under clause 9 shall apply. For the purposes of clause 9(a), Drata has Customer's general authorization to engage Subprocessors in accordance with section 7 of this DPA. Drata shall make available to Customer the current list of Subprocessors in accordance with section 7 of this DPA. Where Drata enters into the EU P-to-P Transfer Clauses with a Subprocessor in connection with the provision of the Services, Customer hereby grants Drata and Drata's Affiliates authority to provide a general authorization on Controller's behalf for the engagement of subprocessors by Subprocessors engaged in the provision of the Services, as well as decision making and approval authority for the addition or replacement of any such subprocessors.

1.7. **Notification of New Subprocessors and Objection Right for new Subprocessors**. Pursuant to clause 9(a), Customer acknowledges and expressly agrees that Drata may engage new Subprocessors as described in section 7 of this DPA. Drata shall inform Customer of any changes to Subprocessors following the procedure provided for in section 7 of this DPA.

1.8. **Complaints - Redress**. Drata shall inform Customer if it receives a Data Subject Request with respect to Personal Data and shall without undue delay communicate the complaint or dispute to Customer. Drata shall not otherwise have any obligation to handle the request (unless otherwise agreed with Customer). The option under clause 11 shall not apply.

1.9. **Liability**. Drata's liability under clause 12(b) shall be limited to any damage caused by its Processing where Drata has not complied with its obligations under the GDPR specifically directed to Processors, or where it has acted outside of or contrary to lawful instructions of Customer, as specified in Article 82 GDPR.

1.10. **Supervision**. Clause 13 shall apply as follows:

1.10.1. Where Customer is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by Customer with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.

1.10.2. Where Customer 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 shall act as competent supervisory authority.

1.10.3. Where Customer is established in the United Kingdom or falls within the territorial scope of application of UK Data Protection Laws, the Information Commissioner's Office shall act as competent supervisory authority.

1.10.4. Where Customer is established in Switzerland or falls within the territorial scope of application of Swiss Data Protection Laws, the Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws.

1.11. **Notification of Government Access Requests**. For the purposes of clause 15(1)(a), Drata shall notify Customer (only) and not the Data Subject(s) in case of government access requests. Customer shall be solely responsible for promptly notifying the Data Subject as necessary.

1.12. **Governing Law**. The governing law for the purposes of clause 17 shall be the law that is designated in the section of the Agreement. If the Agreement is not governed by an EU Member State law, the Standard Contractual Clauses will be governed by either (i) the laws of Ireland; or (ii) where the Agreement is governed by the laws of the United Kingdom, the laws of the United Kingdom.

1.13. **Choice of forum and jurisdiction**. The courts under clause 18 shall be those designated in the Agreement. If the Agreement does not designate an EU Member State court as having exclusive jurisdiction to resolve any dispute or lawsuit arising out of or in connection with this Agreement, the parties agree that the courts of either (i) Ireland; or (ii) where the Agreement designates the United Kingdom as having exclusive jurisdiction, the United Kingdom, shall have exclusive jurisdiction to resolve any dispute arising from the Standard Contractual Clauses. For Data Subjects habitually resident in Switzerland, the courts of Switzerland are an alternative place of jurisdiction in respect of disputes.

1.14. **Data Exports from the United Kingdom and Switzerland under the Standard Contractual Clauses**. In case of any transfers of Personal Data from the United Kingdom and/or transfers of Personal Data from Switzerland subject exclusively to the Data Protection Laws and Regulations of Switzerland ("Swiss Data Protection Laws"), (i) general and specific references in the Standard Contractual Clauses to GDPR or EU or Member State Law shall have the same meaning as the equivalent reference in the Applicable Data Protection Laws of the United Kingdom ("UK Data Protection Laws") or Swiss Data Protection Laws, as applicable; and (ii) any other obligation in the Standard Contractual Clauses determined by the Member State in which the data exporter or Data Subject is established shall refer to an obligation under UK Data Protection Laws or Swiss Data Protection Laws, as applicable. In respect of data transfers governed by Swiss Data Protection

Laws, the Standard Contractual Clauses also apply to the transfer of information relating to an identified identifiable legal entity where such information is protected similarly as Personal Data under Swiss Data Protection Laws until such laws are amended to no longer apply to a legal entity.

1.15. **Conflict**. The Standard Contractual Clauses are subject to this DPA and the additional safeguards set out hereunder. The rights and obligations afforded by the Standard Contractual Clauses will be exercised in accordance with this DPA, unless stated otherwise. In the event of any conflict or inconsistency between the body of this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

2. **ADDITIONAL TERMS FOR THE EU P-TO-P TRANSFER CLAUSES**

For the purposes of the EU P-to-P Transfer Clauses (only), the parties agree the following.

2.1. **Instructions and notifications**. For the purposes of clause 8.1(a), Customer hereby informs Drata that it acts as Processor under the instructions of the relevant Controller in respect of Personal Data. Customer warrants that its Processing instructions as set out in the Agreement and this DPA, including its authorizations to Drata for the appointment of Subprocessors in accordance with this DPA, have been authorized by the relevant Controller. Customer shall be solely responsible for forwarding any notifications received from Drata to the relevant Controller where appropriate.

2.2. **Security of Processing**. For the purposes of clause 8.6(c) and (d), Drata shall provide notification of a personal data breach concerning Personal Data Processed by Drata to Customer.

2.3. **Documentation and Compliance**. For the purposes of clause 8.9, all enquiries from the relevant Controller shall be provided to Drata by Customer. If Drata receives an enquiry directly from a Controller, it shall forward the enquiry to Customer and Customer shall be solely responsible for responding to any such enquiry from the relevant Controller where appropriate.

2.4. **Data Subject Rights**. For the purposes of clause 10 and subject to section 3 of this DPA, Drata shall notify Customer about any request it has received directly from a Data Subject without obligation to handle it (unless otherwise agreed), but shall not notify the relevant Controller. Customer shall be solely responsible for cooperating with the relevant Controller in fulfilling the relevant obligations to respond to any such request.

SCHEDULE 2

DESCRIPTION OF PERSONAL DATA PROCESSING

This Schedule forms part of the Standard Contractual Clauses and must be completed and signed by the parties. As evidenced by the signature of each party's authorized representative below, the data Processing activities carried out by Drata under the Agreement may be described as follows:

1. **Subject Matter.** The parties acknowledge and agree that the subject matter of the Processing is data importer's provision of the Services to data exporter as fully described in this DPA and/or the Agreement.

2. **Duration.** The duration of the Processing of Customer Personal Data is for the Term or until the disposal of all Personal Data, whichever is later.

3. **Nature and Purpose.**

   The nature and purpose of the Processing of Personal Data is for data importer's provision of the Services to data exporter.

4. **Data Categories.** Categories of personal data are identification and contact data (for example, name, address, title, contact details), employment details (for example, employer, job title, geographic location and area of responsibility), and IT information (for example, IP addresses, usage data, cookies data, device specific information, connection data and location data) of the data subjects.

5. **Special Data Categories.** Data exporter is prohibited from providing data importer with sensitive personal information (such as financial, medical or other sensitive personal information such as government IDs, passport numbers or social security numbers), and data importer has no obligation to comply with the DPA with respect to such data.

6. **Data Subjects.** The employees of data exporter.

IN WITNESS WHEREOF, the undersigned have executed this Schedule 2 by their duly authorized representatives, with the intention to be legally bound.

[Customer]	DRATA INC.
(DATA EXPORTER)	(DATA IMPORTER)
By: _____	By: DocuSigned by: Adam Markowitz FE45BCC0E8C1435...
Print Name: _____	Print Name: Adam Markowitz
Title: _____	Title: CEO
Date: _____	Date: 5/2/2022

SCHEDULE 3

CALIFORNIA SCHEDULE

1. For purposes of this Schedule 2, the terms "business," "commercial purpose," "sell" and "service provider" shall have the respective meanings given thereto in the CCPA, and "personal information" shall mean Personal Data that constitutes personal information, the Processing of which is governed by the CCPA.

2. It is the parties' intent that with respect to any personal information, Drata is a service provider. Drata shall (i) not "sell" (as defined in the CCPA) personal information; and (ii) not retain, use or disclose any personal information for any purpose other than for the specific purpose of providing the Services, including retaining, using or disclosing personal information for a commercial purpose (as defined in the CCPA) other than providing the Services. For the avoidance of doubt, the foregoing prohibits Drata from retaining, using or disclosing personal information outside of the direct business relationship between Drata and Customer. Drata hereby certifies that it understands the obligations under this section 2 and shall comply with them.

3. The parties acknowledge that Drata's retention, use and disclosure of personal information authorized by Customer's instructions documented in the DPA are integral to Drata's provision of the Services and the business relationship between the parties.

SCHEDULE 4

Security Measures

1. Organizational management and dedicated staff responsible for the development, implementation and maintenance of the Drata's information security program.

2. Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to Drata's organization, monitoring and maintaining compliance with the Drata's policies and procedures, and reporting the condition of its information security and compliance to internal senior management.

3. Data security controls which include, at a minimum, logical segregation of data, restricted (e.g. role-based) access and monitoring, and utilization of commercially available industry standard encryption technologies for Personal Data that is transmitted over public networks (i.e. the Internet) or when transmitted wirelessly or at rest or stored on portable or removable media (i.e. laptop computers, CD/DVD, USB drives, back-up tapes).

4. Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (e.g. granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all users, periodic review and revoking/changing access promptly when employment terminates or changes in job functions occur).

5. Password controls designed to manage and control password strength, expiration and usage including prohibiting users from sharing passwords and requiring that the Drata's passwords that are assigned to its employees: (i) be at least eight (8) characters in length, (ii) not be stored in readable format on the Drata's computer systems; (iii) must have defined complexity; (iv) must have a history threshold to prevent reuse of recent passwords; and (v) newly issued passwords must be changed after first use.

6. System audit or event logging and related monitoring procedures to proactively record user access and system activity.

7. Physical and environmental security of data centers, server room facilities and other areas containing Personal Data designed to: (i) protect information assets from unauthorized physical access, (ii) manage, monitor and log movement of persons into and out of the Drata's facilities, and (iii) guard against environmental hazards such as heat, fire and water damage.

8. Operational procedures and controls to provide for configuration, monitoring and maintenance of technology and information systems, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from the Drata's possession.

9. Change management procedures and tracking mechanisms designed to test, approve and monitor all material changes to the Drata's technology and information assets.

10. Incident management procedures design to allow Drata to investigate, respond to, mitigate and notify of events related to the Drata's technology and information assets.

11. Network security controls that provide for the use of enterprise firewalls and layered DMZ architectures, and intrusion detection systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.

12. Vulnerability assessment, patch management and threat protection technologies, and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.

13. Business resiliency/continuity and disaster recovery procedures designed to maintain service and/or recovery from foreseeable emergencies or disasters.