Everlaw

Customer Data Processing Addendum

Last Updated: June 28, 2024

This Data Processing Addendum ("DPA") is incorporated into the written agreement that Customer has entered into with Everlaw, Inc. and/or its Affiliates (collectively, "Everlaw") governing Customer's use of the Service (the "Agreement"). Any terms used in this DPA and not defined will have the meanings given to them in the Agreement.

1. **RELATIONSHIP OF THE PARTIES.**

    1.1. **Everlaw.** Everlaw will process the Customer Data as a processor or sub-processor (as applicable) on behalf of Customer (whether the controller or itself a processor acting on behalf of a third party controller). For the purposes of the CCPA (where applicable), Everlaw will process Customer Data as a service provider for the Customer as a business.

    1.2. **Customer.** Customer agrees that it has entered into this DPA on its own behalf and on behalf of the Authorized Controllers, provided that such Authorized Controllers have not entered into their own separate agreement with Everlaw.

2. **DURATION.** This DPA will remain in effect until, and automatically expire upon, deletion of all Customer Data by Everlaw as described in this DPA.

3. **PROCESSING INSTRUCTIONS.**

    3.1. **Customer's Instructions.** Everlaw will process Customer Data under and in accordance with Customer's documented instructions, unless Everlaw believes that any data processing instruction from Customer violates Applicable Privacy Law, in which case Everlaw will notify Customer, unless legally prohibited to do so, before such other processing. For these purposes, Customer instructs Everlaw to process Customer Data: (A) to provide, maintain, and improve the Service in accordance with the Agreement; (B) as further specified via Customer's use of the

Service (*e.g.* including on Customer's account settings page and other functionality of the Service); and (C) as documented in the Agreement and this DPA.

3.2. **Permissible and Non-Permissible Use of Customer Data.** Customer and Everlaw agree that: (A) Everlaw will not retain, use, or disclose Customer Data other than as permitted under the Agreement and Applicable Privacy Law; (B) Everlaw will not sell Customer Data within the meaning of the CCPA or otherwise; (C) Everlaw will not retain, use, or disclose Customer Data outside of the direct business relationship between Customer and Everlaw except as authorized under this DPA; and (D) Everlaw may de-identify or anonymize Customer Data in the course of providing the Service.

3.3. **Customer as Processor.** Where Customer is itself a processor of Customer Data: (A) Customer represents and warrants to Everlaw that the processing instructions in this DPA reflect and do not conflict with the instructions of the third party controllers; and (B) Customer will serve as the sole point of contact for Everlaw with regard to any such third parties.

4. **CUSTOMER'S RESPONSIBILITIES.**

4.1. **Sole Responsibility.** Customer is solely responsible for obtaining and maintaining all the necessary consents prior to accessing, storing, uploading, processing, or storing the Customer Data in the Service.

4.2. **Representations and Warranties.** Customer represents and warrants that: (A) it has provided, and will continue to provide, all notices and has obtained, and will continue to obtain, all consents, permissions, and rights necessary under applicable laws for Everlaw to lawfully process Customer Data for the purposes contemplated by the Agreement; (B) it has complied with all applicable laws, rules, and regulations in the collection and provision of Customer Data to Everlaw and its Sub-processors; and (C) it will ensure its processing instructions comply with applicable laws, rules, and regulations and that the processing of Customer Data by Everlaw in accordance with Customer's instructions will not cause Everlaw to be in breach of Applicable Privacy Law.

5. **AUTHORIZED CONTROLLERS.**

5.1. **Agreement.** Customer will require each Authorized Controller to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Controller is not and does not become a party to the Agreement, and is only a party to the DPA. All access to and use of the Service by Authorized Controllers must comply with the Agreement, and any violation of the Agreement by an Authorized Controller will be deemed a violation by the Customer.

5.2. **Communications.** Customer will remain responsible for coordinating communications with Everlaw under this DPA and be entitled to make and receive communications in relation to this DPA on behalf of each Authorized Controller.

5.3. **Rights and Remedies.** Customer will be solely entitled to exercise the rights and remedies under this DPA, and where Applicable Privacy Law gives an Authorized Controller the ability to exercise a right or seek a remedy under this DPA against Everlaw itself, the parties agree that: (A) solely Customer will exercise any such right or seek any such remedy on behalf of the Authorized Controller; and (B) Customer will exercise any such rights under this DPA in a combined manner for itself and all Authorized Controllers together.

6. **DATA DELETION.**

6.1. **Deletion During Subscription.** Customer may delete or export any Customer Data during the term of the Subscription in a manner consistent with the functionality of the Service. If Customer deletes any Customer Data during the term of the Subscription, such action will constitute an instruction to Everlaw to delete the relevant Customer Data from Everlaw's systems or that is otherwise still in its possession or control.

6.2. **Deletion After Termination.** Termination or expiration of the term of a Subscription serves as Customer's instruction to Everlaw to delete all Customer Data, including copies, still in its possession or control. Customer may export, alone or with Everlaw's support, all Customer Data, within a 30 day grace period following such termination or expiration.

6.3. **Instruction.** Everlaw will comply with Customer's instruction under Sections 6.1 (Deletion During Subscription) and 6.2 (Deletion After Termination) within a commercially reasonable timeframe, except that this requirement will not apply to the extent Everlaw is

required to retain some or all of the Customer Data as required by applicable law.

7. **SECURITY.**

7.1. **Security Measures.** Everlaw will implement and maintain Security Measures designed to protect Customer Data from Security Incidents and to preserve the security and confidentiality of Customer Data. Everlaw will ensure that any person who is authorized by Everlaw to process Customer Data will be under an appropriate obligation of confidentiality, whether contractual or statutory duty.

7.2. **Security Incident Response.** Upon becoming aware of a verified Security Incident, Everlaw will notify Customer without undue delay and: (A) provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer; and (B) promptly take steps, deemed necessary and reasonable by Everlaw, to contain, investigate, and remediate any Security Incident, to the extent that the remediation is within Everlaw's reasonable control. Everlaw's notification of or response to a Security Incident under this Section 7.2 will not be construed as an acknowledgment by Everlaw of any fault or liability with respect to the Security Incident. These obligations will not apply to Security Incidents to the extent they are caused by Customer or its Authorized Users.

7.3. **Updates to Security Measures.** Customer acknowledges that the Security Measures are subject to technical progress and development and that Everlaw may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the material degradation of the overall security of the Service purchased by the Customer.

7.4. **Customer Responsibilities.** Without prejudice to Everlaw's obligations under Sections 7.1 (Security Measures), 7.2 (Security Incident Response), and 7.3 (Updates to Security Measures), Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Service, including securing its account authentication credentials, protecting the security of Customer Data when in transit to and from the Service, and taking any appropriate steps to securely encrypt or backup any Customer Data.

7.5. **Customer's Security Assessment.** Customer agrees, based on its current and intended use of the Service, that the Service, Security Measures, and any other additional security controls described in this DPA: (A) meet Customer's needs, including with respect to any security obligations of Customer under Applicable Privacy Law; and (B) provide a level of security appropriate to the risk regarding the Customer Data.

8. **AUDITS AND DEMONSTRATION OF COMPLIANCE.**

8.1. **Security Reports.** Upon Customer's written request, Everlaw will supply Customer with a summary copy, on a confidential basis, of its most recent Report so that Customer can verify Everlaw's compliance with this DPA. Additionally, upon request and with 90 days' advance notice, and no more than once per calendar year, Everlaw will complete a Customer provided information security program questionnaire relating to the Service provided to Customer.

8.2. **Customer's Audit Rights.** In addition, if required by Applicable Privacy Laws, Everlaw will make available to Customer all information reasonably necessary to demonstrate compliance with this DPA and allow for and contribute to audits, including inspections (which will be conducted at a mutually agreeable time and place) by Customer to assess compliance with this DPA, provided that such audit or inspection will: (A) take place not more than once per calendar year and at Customer's expense; and (B) be conducted during normal business hours in a manner that will not interfere with Everlaw's normal business activities. Notwithstanding the foregoing, Customer may also exercise its audit rights when Customer is expressly requested or required to provide this information to a supervisory authority or when Everlaw has experienced a Security Incident.

8.3. **Everlaw's Information.** Nothing in this DPA will be construed to require Everlaw to provide: (A) trade secrets or any proprietary information; (B) any information that would violate Everlaw's confidentiality obligations, contractual obligations, or applicable law; or (C) any information, the disclosure of which could threaten, compromise, or otherwise put at risk the security, confidentiality, or integrity of Everlaw's infrastructure, networks, systems, or data.

8.4. **Exceptions.** Nothing in this Section 8 varies or modifies any rights or obligations of Customer or Everlaw under the SCCs where Section 10.3 (SCCs) applies.

9. **RIGHTS OF DATA SUBJECTS AND COOPERATION.**

9.1. **Data Subject Request.** Customer will respond to any requests from data subjects or applicable supervisory authorities relating to the processing of Customer Data under the Agreement. To the extent Customer is unable to independently retrieve, access, or delete the relevant Customer Data within the Service in order to respond to such requests, Everlaw will (at Customer's cost and taking into account the nature of the processing) provide all reasonable cooperation to assist Customer by appropriate technical and organizational measures, to the extent possible. In the event that any such request is made to Everlaw directly, Everlaw will not respond to such request directly without Customer's prior authorization, unless legally compelled to do so. If Everlaw is required to respond to such a request, Everlaw will promptly notify Customer and provide it with a copy of the request, unless legally prohibited to do so.

9.2. **Data Protection Impact Assessment.** To the extent Everlaw is required under Applicable Privacy Law, Everlaw will provide reasonably requested information regarding Everlaw processing of Customer Data under the Agreement, to the extent Customer does not otherwise have access to the relevant information and to the extent that such information is available to Everlaw, to enable the Customer to carry out data protection impact assessments or prior consultations with supervisory authorities as required by applicable law.

10. **CROSS-BORDER DATA TRANSFERS.**

10.1. **Principal Place of Processing.** Customer may choose within which of Everlaw's available AWS instances to have its Customer Data stored and processed. Notwithstanding the foregoing, Customer acknowledges that Everlaw may in connection with the performance of the Service and the processing activities described in Schedules 1 and 2 of this DPA, need to transfer and process Customer Data and Controller Data to and in the US and anywhere else in the world where Everlaw or its Sub-processors maintain data processing operations. Everlaw will ensure such transfers are made

in compliance with the requirements of Applicable Privacy Law and this DPA.

10.2. **Data Privacy Framework.** Everlaw complies with the Data Privacy Framework in relation to transfers from the EEA, UK, and Switzerland to the U.S. The parties agree that Everlaw shall use the Data Privacy Framework to lawfully receive Customer Data and Controller Data in the U.S. and Everlaw shall ensure that it provides at least the same level of protection to such data as is required by the Data Privacy Framework Principles. Everlaw shall notify Customer if it makes a determination that it can no longer comply with its obligations under the Data Privacy Framework.

10.3. **SCCs.** In the event that the Data Privacy Framework is invalidated, or the Data Privacy Framework does not otherwise apply to the transfer of Personal Data, then to the extent the transfer of Personal Data from Customer to Everlaw is a Restricted Transfer, the parties agree to be subject to, abide by, and process such Personal Data in compliance with the SCCs as follows:

10.3.1. **EEA Transfers.** In relation to Personal Data that is protected by the EU GDPR, the SCCs will apply as follows: (A) Everlaw will be the "data importer" and Customer will be the "data exporter"; (B) Module One will apply to Controller Data and Modules Two or Three (as appropriate) will apply to Customer Data; (C) in Clause 7, the optional docking clause will apply; (D) in Clause 9 of Modules Two and Three, Option 2 will apply and the time period for prior notice of Sub-processor changes is identified in Section 11 (Sub-processing) of this DPA; (E) in Clause 11, the optional language will not apply; (F) in Clause 17, Option 1 will apply, and the SCCs will be governed by Irish law; (G) in Clause 18(b), disputes will be resolved before the courts of Ireland; (H) Annex I will be deemed completed with the information set out in Schedule 1 and Schedule 2 of this DPA; and (I) Annex II will be deemed completed with the information stated in Schedule 3 of this DPA.

10.3.2. **Swiss Transfers.** In relation to Personal Data that is protected by the Swiss FADP, the SCCs as implemented under Section 10.3.1 (EEA Transfers) will apply with the following modifications: (A) references to "Regulation (EU) 2016/679" are interpreted as references to the Swiss FADP;

(B) references to specific Articles of "Regulation (EU) 2016/679" are replaced with the equivalent article or section of the Swiss FADP; (C) references to "EU," "Union," and "Member State" are replaced with "Switzerland"; (D) Clause 13(a) and Part C of Annex II are not used and references to the "competent supervisory authority" and "competent courts" will be interpreted as references to the "Swiss Federal Data Protection and Information Commissioner" and the "competent Swiss courts"; (E) in Clause 17, the SCCs are governed by the laws of Switzerland; and (F) in Clause 18(b), disputes will be resolved before the competent courts of Switzerland.

10.3.3. **UK Transfers.** In relation to Personal Data that is protected by the UK GDPR, the SCCs as implemented under Section 10.3.1 (EEA Transfers) will apply with the following modifications: (A) the SCCs are deemed amended as specified by the UK Addendum, which is deemed executed between the parties; (B) any conflict between the SCCs and the UK Addendum will be resolved in accordance with Section 10 and Section 11 of the UK Addendum; (C) Tables 1 to 3 in Part 1 of the UK Addendum are deemed completed using the information contained in the Schedules of this DPA; and (D) Table 4 in Part 1 of the UK Addendum is deemed completed by selecting "neither party."

10.3.4. Where this Section 10.3 applies, it is not the intention of either party to contradict or restrict any of the provisions stated in the SCCs, and, accordingly, if and to the extent the SCCs conflict with any provision of the Agreement (including this DPA), the SCCs will prevail to the extent of such conflict.

11. **SUB-PROCESSING.**

11.1. **Authorized Sub-processors.** Customer agrees to provide a general authorization to Everlaw to engage Sub-processors to process Customer Data on Customer's behalf. Everlaw will notify Customer if it adds or replaces any Sub-processors at least 10 days in advance of any such changes.

11.2. **Sub-processors' Obligations.** Everlaw will: (A) enter into a written agreement with each Sub-processor containing terms that provide

at least the same level of protection for Customer Data as those contained in this DPA, to the extent applicable to the nature of the services provided by such Sub-processor; and (B) remain responsible for all obligations sub-contracted and for any acts or omissions of the Sub-processor.

11.3. **Objection to Sub-processors.** Customer may object, in writing, to Everlaw's appointment of a new Sub-processor on reasonable grounds relating to data protection (e.g. if making Customer Data available to the Sub-processor may violate Applicable Privacy Law) by notifying Everlaw in writing within 15 calendar days of receipt of Everlaw's notice. Customer's notice must explain the reasonable grounds for the objection, and the parties will discuss such concerns with a view to achieving commercially reasonable resolution. If no such resolution can be reached, Everlaw will, at its sole discretion, either not appoint that proposed Sub-processor in respect of that Customer Data only or permit Customer in writing to suspend or terminate the affected Service in accordance with the termination provisions in the Agreement without liability to either party (but without prejudice to any fees incurred by Customer prior to suspension or termination). If Customer does not object as described above, silence will be deemed approval.

12. **LIMITATION OF LIABILITY.**

12.1. **EXCLUSION OF DAMAGES.** EACH PARTY AND ITS RESPECTIVE AFFILIATES' LIABILITY, TAKEN TOGETHER IN THE AGGREGATE, ARISING OUT OF OR RELATED TO THIS DPA (INCLUDING THE SCCS) WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), OR UNDER ANY OTHER THEORY OF LIABILITY, WILL BE SUBJECT TO THE LIMITATIONS AND EXCLUSIONS OF LIABILITY IN THE AGREEMENT, AND ANY REFERENCE IN PROVISIONS TO THE LIABILITY OF A PARTY MEANS THE AGGREGATE LIABILITY OF THAT PARTY AND ALL OF ITS AFFILIATES UNDER AND IN CONNECTION WITH THE AGREEMENT AND THIS DPA TOGETHER.

12.2. **MAXIMUM AGGREGATE LIABILITY.** EVERLAW'S TOTAL AGGREGATE LIABILITY FOR ALL CLAIMS FROM CUSTOMER AND ALL AUTHORIZED CONTROLLERS ARISING OUT OF OR RELATED TO THE AGREEMENT OR THIS DPA, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), OR UNDER ANY OTHER THEORY OF LIABILITY, WILL APPLY IN AGGREGATE FOR ALL CLAIMS ARISING UNDER OR IN CONNECTION WITH BOTH THE AGREEMENT AND

THIS DPA, INCLUDING BY CUSTOMER AND ALL AUTHORIZED CONTROLLERS, AND IN PARTICULAR WILL NOT BE UNDERSTOOD TO APPLY INDIVIDUALLY AND SEVERALLY TO CUSTOMER AND/OR TO ANY AUTHORIZED CONTROLLER THAT IS A PARTY TO THIS DPA.

13. **MISCELLANEOUS.**

13.1. **Order of Agreements.** Notwithstanding anything to the contrary in the Agreement, to the extent of any conflict or inconsistency between this DPA and the remaining terms of the Agreement, this DPA will govern.

13.2. **Governing Law.** This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless otherwise required by Applicable Privacy Law or the SCCs.

13.3. **Permitted Disclosures.** Each party acknowledges that the other party may disclose the SCCs, this DPA, and any privacy–related provisions in the Agreement to any appropriate regulator upon request.

14. **DEFINITIONS.**

14.1. **Applicable Privacy Law** means all applicable data protection and privacy laws, regulations, guidance, or codes of practice relating to the processing of Customer Data in connection with the Agreement.

14.2. **Authorized Controller** means the Customer and, to the extent required under Applicable Privacy Law, its Affiliates and any Authorized Users who are also controllers of the Customer Data and permitted to use the Service as Authorized Users.

14.3. **CCPA** means the California Consumer Privacy Act of 2018 (California Civil Code §§ 1798.100-1798.199), including any amendments and its implementing regulations from time to time.

14.4. **Controller Data** means the Personal Data that Everlaw processes as a controller under the Agreement, as described in Schedule 1.

14.5. **Customer Data** means the Personal Data included in Customer's Case Materials that Everlaw processes on behalf of Customer under the Agreement, as described in Schedule 2.

14.6. **Data Privacy Framework** means (as applicable) the EU-U.S. Data Privacy Framework, the Swiss-U.S. Data Privacy Framework, and

the UK Extension to the EU-U.S. Data Privacy Framework self-certification programs operated by the U.S. Department of Commerce, and their respective successors.

14.7. **Data Privacy Framework Principles** means the Principles and Supplemental Principles contained in the relevant Data Privacy Framework, as may be amended, superseded, or replaced.

14.8. **EEA** means the European Economic Area.

14.9. **EU GDPR** means 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, and repealing Directive 95/46/EC.

14.10. **Personal Data** means any information which is protected as "personal data," "personal information," or "personally identifiable information" under Applicable Privacy Law.

14.11. **Report** means Everlaw's Service Organizational Control (SOC) 2 Report or comparable reports.

14.12. **Restricted Transfer** means: (A) where the EU GDPR applies, a transfer of Personal Data from the EEA to a country outside the EEA which is not subject to an adequacy determination by the European Commission; (B) where the UK GDPR applies, a transfer of Personal Data from the UK to any other country which is not based on adequacy regulations under the UK GDPR, and (C) where the Swiss FADP applies, a transfer of Personal Data from Switzerland to any other country which is not based on an adequacy decision recognized under Swiss data protection law, in any case whether such transfer is direct or via onward transfer.

14.13. **Security Incident** means a breach of Everlaw's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data transmitted, stored, or otherwise processed by Everlaw and/or its Sub-processors in connection with the provision of the Service.

14.14. **Security Measures** means the appropriate technical and organizational measures Everlaw implements and maintains as described in Schedule 3.

14.15. **Service** for the purposes of this DPA means either the Service or Storybuilder Service, each as defined in the applicable Agreement.

14.16. **SCCs** means the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021, as amended, superseded, or replaced from time to time.

14.17. **Sub-processor** means any third party processor that has access to Customer Data and that is engaged by Everlaw to assist in fulfilling its obligations with respect to providing the Service under the Agreement. Sub-processors may include third parties but excludes any Everlaw employee, contractor, or consultant. A current list of Everlaw's Sub-processors is available at: www.everlaw.com/legal/list-of-subprocessors.

14.18. **Swiss FADP** means the Swiss Federal Act on Data Protection of 2020 and its corresponding ordinances.

14.19. **UK** means the United Kingdom.

14.20. **UK Addendum** means the International Data Transfer Addendum (version B1.0) issued by the Information Commissioner's Office under s.119(A) of the UK Data Protection Act 2018, as amended, superseded, or replaced from time to time.

14.21. **UK GDPR** means, collectively, the EU GDPR as saved into UK law by virtue of Section 3 of the UK's European Union (Withdrawal) Act 2018 and the UK Data Protection Act 2018.

14.22. The terms "personal data," "data subject," "supervisory authority," "processing" (including the terms "process," "processes," and "processed" and other variations), "controller," and "processor" as used in this DPA have the meanings given to them in Applicable Privacy Law.

14.23. The terms "business" and "service provider" have the meanings given to them in the CCPA.

SCHEDULE 1 (Controller Data)

Description of Processing Activities / Transfer

Annex 1(A) List of Parties:

DATA EXPORTER	**DATA IMPORTER**
Name: The party named as Customer in the Order	Name: Everlaw, Inc.

Form	
Address: The Customer's address as identified in the Order Form	Address: 2101 Webster Street, Ste 1500 Oakland, California 94612, United States
Contact person's name, position and contact details: The Customer's Commercial Contact information as identified in the Order Form	Contact person's name, position and contact details: Everlaw, Inc., Attn: Privacy, 2101 Webster Street, Ste 1500, Oakland, California 94612, United States, privacy@everlaw.com
Activities relevant to the transfer: See Annex 1(B) below	Activities relevant to the transfer: See Annex 1(B) below
Role: Controller	Role: Controller

Annex 1(B) Description of transfer / processing activities:

	DESCRIPTION
Categories of data subjects:	Authorized Users, as defined in the Agreement.
Categories of personal data:	The categories of Personal Data include: Account Information (e.g. name, job title, email address, mailing address, phone number, employer's name, login credentials, contact preferences for marketing information, billing information associated with Customer's account); Service-Generated Data (e.g. diagnostic, capacity and usage information, log files, IP address, address(es) of the web page(s) visited, browser type and settings, information about activity in the Service, privacy and security settings); Support Data (e.g. account preferences, data provided when Authorized Users contact Everlaw for help, contact or

	authentication data, the content of chats and other communications); Other Personal Data (if any) collected by Everlaw in connection with the Service and which Everlaw processes as a controller, as more particularly described in the Privacy Notice available at https://www.everlaw.com/legal/privacy-notice/.
Sensitive data:	N/A.
If sensitive data, the applied restrictions or safeguards	N/A.
Frequency of the transfer:	Continuous.
Nature and subject matter of processing:	The nature and subject matter of Everlaw's processing include: (A) to provide, improve, update, maintain, and protect the Service; (B) to respond to requests, comments, and questions; (C) for transactional and administrative matters; (D) to comply with legal obligations; (E) to send service-related emails, marketing communications, and other non-marketing communications; (F) to develop and improve Everlaw's marketing activities; (G) to provide customer support and answer support requests; and (H) for all other purposes as more particularly described in the Privacy Notice available at https://www.everlaw.com/legal/privacy-notice.
Purpose(s) of the data transfer and further processing:	Everlaw is headquartered in the United States and has offices, employees, and service providers who operate around the globe. As a global business, Everlaw may process Controller Data in locations outside of the country where the data subject is located because Controller Data is typically processed by centralized or regionalized operations like billing, support, and security. For more

	information, see the Privacy Notice available at https://www.everlaw.com/legal/privacy-notice.
Retention period (or, if not possible to determine, the criteria used to determine that period):	Everlaw will not, and will not permit any third party to, retain the Controller Data for longer than the period during which Everlaw has a legitimate need to retain the Controller Data for the purposes it is processed and in compliance with Applicable Privacy Law.

Annex 1(C) Competent supervisory authority:

For the purposes of the SCCs, the competent supervisory authority will be determined in accordance with the EU GDPR, UK GDPR, or Swiss FADP, as applicable.

SCHEDULE 2 (Customer Data)

Description of the Processing Activities / Transfer

Annex 1(A) List of Parties:

DATA EXPORTER	DATA IMPORTER
Name: The party named as Customer in the Order Form	Name: Everlaw, Inc.
Address: The Customer's address as identified in the Order Form	Address: 2101 Webster Street, Ste 1500 Oakland, California 94612, United States
Contact person's name, position and contact details: The Customer's Commercial Contact information as identified in the Order Form	Contact person's name, position, and contact details: Everlaw, Inc., Attn: Privacy, 2101 Webster Street, Ste 1500, Oakland, California 94612, United States, privacy@everlaw.com

Activities relevant to the transfer: See Annex 1(B) below	Activities relevant to the transfer: See Annex 1(B) below
Role: Controller or processor	Role: Processor

Annex 1(B) Description of Transfer / Processing Activities:

	DESCRIPTION
Categories of data subjects:	Individuals whose Personal Data is included in Case Materials.
Categories of personal data:	Any Personal Data included in Case Materials that Customer, Authorized Users, or third parties acting on Customer's behalf, may submit, upload, or otherwise provide to the Service, the extent of which is exclusively determined and controlled by the Customer.
Sensitive data:	Customer, Authorizer Users, or third parties acting on Customer's behalf, may submit Personal Data that contains special categories of data to Everlaw in connection with the performance of the Service, the extent of which is exclusively determined and controlled by the Customer.
If sensitive data, the applied restrictions or safeguards:	See Schedule 3 for applied restrictions and safeguards.
Frequency of the transfer:	Continuous.
Nature and subject matter of processing:	Providing the Service to Customer. Customer Data transferred will be processed in accordance with the Agreement and may be subject to the following processing activities: (A) storage and other processing necessary to provide, maintain, and improve the Service, as applicable, provided to Customer; and/or (B)

	disclosures in accordance with the Agreement and/or as compelled by applicable laws.
Duration of the processing:	Personal Data will be processed in accordance with Sections 2 and 6 of this DPA.
Purpose(s) of the data transfer and further processing:	Everlaw may process Customer Data: (A) as necessary to provide, maintain, and improve the Service as applicable to Customer and in accordance with the Agreement, including analytical capabilities native to the Everlaw platform, data analysis for the purposes of diagnosing support requests and debugging platform issues, and, where appropriate, the resolution and reporting on the support requests; (B) to perform any steps necessary for the performance of the Agreement; and (C) to comply with other reasonable instructions provided by Customer (e.g. via email) that are consistent with this DPA or the Agreement.
Retention period (or, if not possible to determine, the criteria used to determine that period):	In accordance with Section 6 of the DPA.

Annex 1(C) Competent supervisory authority:

For the purposes of the SCCs, the competent supervisory authority will be determined in accordance with the EU GDPR, UK GDPR, or Swiss FADP, as applicable.

SCHEDULE 3

Everlaw Security Measures

Everlaw has implemented and will maintain security measures, internal controls, and information security policies and procedures designed to protect Customer Data (collectively, the "Security Measures"). Everlaw regularly monitors compliance with these safeguards. Everlaw may update the Security Measures from time to time and without notice, provided that such updates

and modifications do not materially decrease the overall security of the Service during the term of the Subscription.

The following Security Measures are in place to protect the Customer Data processed by Everlaw on behalf of Customer:

Measures of pseudonymization and encryption of Customer Data

- Everlaw requires full-disk hard drive encryption using AES-256 for all employee computers, and uses role-based access control ("RBAC"), multi-factor authentication ("MFA"), and account management procedures to control access to Customer Data.
- Everlaw encrypts data in transit and at rest using hybrid encryption techniques that constitute software-based encryption, hosting solutions (e.g. Amazon Web Services ("AWS")), and self-encrypting drives to align with NIST Special Publication 800-53.
- Customer Data at rest is encrypted using the AES-256 algorithm.
- Everlaw uses Transport Layer Security ("TLS") protocol version 1.2 or higher to protect HTTPS communications.
- For email security, Everlaw leverages opportunistic TLS encryption (OE) by default.
- Customer Data that resides in AWS is encrypted at rest as stated in AWS's documentation and whitepaper. Further information about AWS's security practices can be found at https://aws.amazon.com/compliance/data-center/controls/.
- AWS log-in credentials and private keys generated by the Service are for Everlaw's internal use only.
- Encryption keys are rotated at least annually.

Measures for ensuring ongoing confidentiality, integrity, availability, and resilience of processing systems and services

- Everlaw maintains a record of personnel authorized to access systems that contain Customer Data.
- Privileged access requires a formal account management and access control procedure that requires review and approval from a line manager or other executives, as dictated by Everlaw's information security policies.
- Everlaw deactivates authentication credentials of individuals promptly following the date of their employment or services termination or a role

transfer that no longer requires access to Customer Data.

- Everlaw's personnel are legally obligated to maintain the confidentiality of Customer Data and this obligation continues even after their employment or services provided end.
- Employees complete mandatory training annually, which covers data privacy and governance, data protection, confidentiality, social engineering, password policies, and information security.
- Everlaw requires difficult-to-guess passwords for all employees and follows NIST best practices.
- Everlaw web application account passwords are hashed using bcrypt when stored.
- Everlaw web application sessions expire after 30 minutes of inactivity to prevent further access to the system.
- The Everlaw web application retains session locks until the session user reestablishes access using Everlaw identification and authorization procedures.

Measures for ensuring the ability to restore the availability and access to Customer Data in a timely manner in the event of a physical or technical incident

- Everlaw maintains geographically-distributed data centers leveraging AWS cloud hosting infrastructure in several jurisdictions, including the United States (US East and West Regions), Canada (Central Region), Australia (Asia Pacific, Sydney Region), the United Kingdom (London Region), and the EU (Frankfurt Region).
- Everlaw's information systems have security controls designed to detect and mitigate attacks by using logs and alerting.
- Everlaw's incident reporting and response procedure aligns with NIST SP 800-61 guidance on handling incidents, including steps for breach notification.
- All incidents are logged in an incident tracking system that is subject to auditing on an annual basis.
- Everlaw has a business continuity and disaster recovery plan that incorporates input from periodic risk assessments, vulnerability scanning, and threat analysis.

- Everlaw conducts an incident response and business continuity and disaster recovery test annually that is used to inform the ongoing risk assessment and management process.

Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures to ensure the security of the processing

- Everlaw conducts regular risk assessments and monitors the effectiveness of its safeguards, controls, and systems, including conducting vulnerability scanning, annual penetration testing, intrusion detection, and continuous monitoring.
- Everlaw's vulnerability management program includes an independent testing team to perform vulnerability scanning and a variety of vulnerability scanning tools to assess its internal and external network environments against emerging security threats.
- Everlaw implements endpoint protection on its hosting environments, including antivirus, which are continuously updated with critical patches or security releases in accordance with Everlaw's Development & Configuration Management Policy.
- The servers that host the Everlaw Service are scanned for viruses and malware on a weekly basis.
- The Everlaw web application, network segmentation, and interconnections are protected by firewalls.
- The Amazon Virtual Private Cloud allows Everlaw services to operate in separate, virtual networks that are isolated from other external traffic.
- Everlaw's corporate equipment is protected to reduce the risks from environmental threats, hazards, and opportunities for unauthorized access.
- Sub-processors undergo onboarding due diligence to ensure compliance with security and privacy requirements, laws, and regulations. In addition and to the extent applicable, sub-processors are required to sign a Data Processing Addendum (DPA) that includes compliance with data protection laws, confidentiality, data retention, and access requirements.

Measures for user identification and authorization

- Everlaw uses commercially reasonable practices to identify and authenticate users who attempt to access information systems. Everlaw's authentication and password protection practices are designed to

maintain the confidentiality and integrity of account credentials when they are assigned and distributed and during storage.

- Customers may set their own password complexity when choosing to enable Single Sign On via the SAML 2.0 protocol.

Measures for the protection of Customer Data during transmission

- Customer Data is encrypted in transit. Encryption is a requirement.
- All communications between the clients and Everlaw, as well as all third-party applications, take place over a secure HTTPS connection using TLS 1.2 protocol to ensure data in transit is encrypted.
- The Everlaw production environments include logical and physical separation of components using networking and software defined networking technologies where appropriate. Production, testing, and staging environments are also logically separated to ensure the security of Customer Data.
- All connections between Everlaw internal networks and the Internet or any other publicly-accessible computer network include an approved firewall or related access control system.

Measures for the protection of Customer Data during storage

- Customer Data is hosted by AWS. Everlaw maintains complete administrative control over its virtual servers.
- AWS Key Management System ("KMS") managed server-side encryption keys are used to encrypt data in our cloud infrastructure. AWS KMS is a secure and resilient service that uses FIPS 140-2 validated hardware security modules to protect keys that cannot be retrieved from the service by anyone or transmitted beyond the AWS regions where they were created.
- Customer Data within Everlaw's multi-tenant environments is logically segregated and attempts to access Customer Data outside allowed domain boundaries are prevented and logged (Customer Data can be logically and physically segregated in accordance with the Customer Agreement).
- Antivirus scans are conducted regularly to detect malicious files present in the production environment and all access to Customer Data is logged.
- Customer Data is protected during storage by AWS endpoint protection, which includes firewalls and antivirus.

Measures for ensuring physical security of locations where Customer Data is processed

- Physical access to data hosting facilities is documented and managed by AWS.
- Everlaw limits access to its corporate offices to identified authorized individuals who require access for the performance of their job function and authorized visitors.
- Policy requires that all visitors to Everlaw's corporate offices are escorted at all times by authorized personnel.
- Physical access to Everlaw corporate offices is managed and administered by the Business Operations team.
- Everlaw uses commercially reasonable systems and measures to protect against loss of data due to power supply failure or disruptions to Everlaw office.
- Access to customer physical media is limited to employees who require access. The Data Operations team administers employees' access, which must be approved based on job role.
- Ad hoc access to customer physical media under specific requests are administered by the Data Operations team with the approval of the employee's supervisor.
- Everyone with access rights to an Everlaw corporate office must sign a non-disclosure agreement.
- Policy requires that access cards and/or keys are not shared or loaned to others without authorization.
- Policy requires that access cards and/or keys that are no longer required are returned to the Facilities team.
- Cards are not reallocated to another individual, bypassing the return process.
- Everlaw employees are responsible for notifying the Facilities team within 24 hours if their access cards and/or keys are lost, stolen or compromised.
- Cards and/or keys have no identifying information coded into them.
- Everlaw maintains an inventory of all customer physical media received by Everlaw. Everlaw imposes restrictions on handling Customer Data and has procedures for disposing of materials that contain Customer Data.

- Everlaw uses commercially reasonable processes to securely destroy customer physical media in accordance with the Customer Agreement.

Measures for ensuring events logging

- Event and system access logs are logged, monitored, and reviewed periodically.
- User activity metrics and logs, configuration changes, deletions, and updates are written automatically to audit logs in operational systems.
- User activity metrics are available to customers within the Everlaw web application.
- Audit logs maintain detailed information such as timestamp, IP address, specific action taken, requested metadata.
- Certain log events on Everlaw such as timestamps, IPs, login/logouts, and errors are available to authorized employees for security investigations.
- Notifications and alerts are sent based on the rules configured in the monitoring systems to identify anomalies, suspicious network behavior, abnormal activities, and potential threats.
- Everlaw has a central Security Information and Event Management (SIEM) system and other product tools to monitor the security alerts generated by the Everlaw Service.

Measures for ensuring system configuration, including default configuration

- Everlaw has a Development & Configuration Management Policy to aid in securely controlling assets, configurations, and changes throughout the software development lifecycle.
- Everlaw monitors changes to in-scope systems to ensure that changes follow the process and to mitigate the risk of undetected changes to the production environment. Changes are tracked in our change management platform.

Measures for internal security governance and IT management

- Everlaw maintains security documents describing its Security Measures and relevant procedures and responsibilities of its personnel. These include a suite of information security policies and procedures, security and privacy training documents, penetration and vulnerability scanning reports, and Service Organization Control (“SOC”) 2 Type 2 (or comparable) reports.

- Everlaw has established an Information Security Management System in accordance with the International Organization for Standardization ("ISO") 27001:2013 standard. Information security-related business operations continue to be carried out in line with the ISO 27001:2013 standard.
- The authority and responsibility for managing Everlaw's information security program has been delegated to the Governance, Risk, and Compliance team, who is authorized by senior management to take actions necessary to establish, implement, and manage Everlaw's information security program.

Measures for certification/assurance of processes and products

- Everlaw's system of internal control requires annual independent third-party audits to test the operational effectiveness of its program and practices. Annual audits include SOC 2 Type 2 (Security, Privacy, Confidentiality & Availability) and ISO 27001.
- In addition Everlaw has engaged independent auditors to review its compliance status for both HIPAA and GDPR, attesting to our commitment to safeguard the confidentiality, integrity, and privacy of information stored and processed in our Service.
- AWS has achieved: (A) SOC 1, 2, and 3; (B) ISO 27001, 27017, 27018, 27701, and 9001; (C) Cloud Security Alliance Security, Trust, Assurance and Risk Cloud Control Matrix v3.0.1; (D) FedRAMP; and (E) uses FIPS 140-2 validated cryptographic modules, in addition to meeting compliance standards for many other legal, security, and privacy frameworks. Further information about AWS' security practices can be found at https://aws.amazon.com/compliance/data-center/controls/.

Measures for ensuring data minimization

- Customer Data collection by Everlaw is limited to the purposes of processing (or the data that the customer chooses to provide).
- Security Measures are in place to provide only the minimum amount of access necessary to perform the Service.

Measures for ensuring data quality

- Everlaw has a process that allows individuals to exercise their privacy rights (including a right to amend and update information), as described in Everlaw's Privacy Notice https://www.everlaw.com/legal/privacy-notice/.

- Software releases and updates/patches to Everlaw production environments are tested for functionality and security, including any significant modifications, major enhancements, and new systems, before deployment.

Measures for ensuring limited data retention

- Customer Data is retained as per the contractual terms agreed with the Customer and as required by applicable privacy law.
- After termination of a Subscription, Customer Data is deleted from the production environment within a commercially reasonable timeframe.

Measures for ensuring accountability

- Events and audit trails related to Everlaw Service and system access are logged, monitored, and reviewed periodically.
- Everlaw adopts the Three Lines of Defense governance model for its system of internal control. This model is designed to ensure the effective and transparent management of compliance obligations and risks by making accountabilities clear across the organization.

Measures for allowing data portability and ensuring erasure

- Customers have the ability to export Customer Data to CSV, PDF, and ZIP formats via the Everlaw web application.
- Everlaw has a process that allows individuals to exercise their privacy rights under Applicable Privacy Law, as described in Everlaw's Privacy Notice https://www.everlaw.com/legal/privacy-notice/.