Grepr

Data Processing Addendum (Last updated August 26th, 2026)

This Data Processing Addendum ("DPA") supplements the Customer Terms and Conditions, Grepr Technology Platform Agreement, or other terms governing (the "Agreement") entered into by and between the Customer identified in an Agreement ("Customer") and Grepr, Inc. ("Grepr") By executing the DPA in accordance with Section 11 herein, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws (defined below), in the name and on behalf of its Affiliates (defined below), if any. This DPA incorporates the terms of the Agreement, and any capitalized terms used herein but not otherwise defined in this DPA shall have the meaning set forth in the Agreement.

1. Definitions

1.1 "Affiliate" means (i) an entity of which a party directly or indirectly owns fifty percent (50%) or more of the stock or other equity interest, (ii) an entity that owns at least fifty percent (50%) or more of the stock or other equity interest of a party, or (iii) an entity which is under common control with a party by having at least fifty percent (50%) or more of the stock or other equity interest of such entity and a party owned by the same person, but such entity shall only be deemed to be an Affiliate so long as such ownership exists.

1.2 "Authorized Subprocessor" means a third-party who has a need to know or otherwise access Customer's Personal Data to enable Grepr to perform its obligations under this DPA or the Agreement, and who is either (1) listed in Exhibit B or (2) subsequently authorized under Section 4.2 of this DPA.

1.3 "Data Exporter" means Customer.

1.4 "Data Importer" means Grepr.

1.5 "Data Protection Laws" means any applicable laws and regulations in any relevant jurisdiction relating to the use or processing of Personal Data including: (i) the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 ("CCPA"), (ii) the General Data Protection Regulation (Regulation (EU) 2016/679) ("EU GDPR") and the EU GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "UK GDPR") (together, collectively, the "GDPR"), (iii) the Swiss Federal Act on Data Protection; (iv) the UK Data Protection Act 2018, (v) the Privacy and Electronic Communications (EC Directive) Regulations 2003; (vi) the Virginia Consumer Data Protection Act ("VCDPA"); (vii) the Colorado Privacy Act ("CPA"); (viii) the Connecticut Data Privacy Act ("CTDPA"), (ix) the Utah Consumer Privacy Act ("UCPA"); and (x) the Washington My Health My Data Act ("MHMDA"), in each case, as updated, amended or replaced from time to time. The terms "Data Subject", "Personal Data", "Personal Data Breach", "processing", "processor," "controller," and "supervisory authority" shall have the meanings set forth in the GDPR.

1.6 "Data Privacy Framework" means, as applicable, EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and/or the Swiss-U.S. Data Privacy Framework.

1.7 "EU SCCs" means, as applicable, the standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021, for transfers of personal data to countries not otherwise recognized as offering an adequate level of protection for personal data by the European Commission (as amended and updated from time to time), as modified by Section 6.2 of this DPA.

1.8 "ex-EEA Transfer" means the transfer of Personal Data, which is processed in accordance with the GDPR, from the Data Exporter to the Data Importer (or its premises) outside the European Economic Area (the "EEA"), and such transfer is not governed by an adequacy decision made by the European Commission in accordance with the relevant provisions of the GDPR. For the avoidance of doubt, an ex-EEA Transfer includes access to Personal Data from outside the EEA, irrespective of the location at which such Personal Data is stored.

1.9 "ex-UK Transfer" means the transfer of Personal Data covered by Chapter V of the UK GDPR, which is processed in accordance with the UK GDPR and the Data Protection Act 2018, from the Data Exporter to the Data Importer (or its premises) outside the United Kingdom (the "UK"), and such transfer is not governed by an adequacy decision made by the Secretary of State in accordance with the relevant provisions of the UK GDPR and the Data Protection Act 2018. For the avoidance of doubt, an ex-UK Transfer includes access to Personal Data from outside the UK, irrespective of the location at which such Personal Data is stored.

1.10"Grepr Account Data" means personal data that relates to Grepr's relationship with Customer, including the names or contact information of individuals authorized by Customer to access Customer's account and billing information of individuals that Customer has associated with its account. Grepr Account Data also includes any

data Grepr may need to collect for the purpose of managing its relationship with Customer, identity verification, or as otherwise required by applicable laws and regulations.

1.11 "Grepr Usage Data" means Service usage data collected and processed by Grepr in connection with the provision of the Services, including without limitation data used to identify the source and destination of a communication, activity logs, and data used to optimize and maintain performance of the Services, and to investigate and prevent system abuse.

1.12 "Services" shall mean providing the Grepr platform as contemplated in the Agreement.

1.13 "Standard Contractual Clauses" means the EU SCCs and the UK SCCs.

1.14 "UK Addendum" has the meaning set forth in Exhibit D.

1.15 "UK SCCs" means, as applicable, the EU SCCs, as amended by the UK Addendum.

2. Relationship of the Parties; Processing of Data

2.1 The parties acknowledge and agree that with regard to the processing of Personal Data, Customer may act either as a controller or processor and, except as expressly set forth in this DPA or the Agreement, Grepr is a processor. Customer shall, in its use of the Services, at all times process Personal Data, and provide instructions for the processing of Personal Data, in compliance with Data Protection Laws. Customer shall ensure that the processing of Personal Data in accordance with Customer's instructions will not cause Grepr to be in breach of the Data Protection Laws. Customer is solely responsible for the accuracy, quality, and legality of (i) the Personal Data provided to Grepr by or on behalf of Customer, (ii) the means by which Customer acquired any such Personal Data, and (iii) the instructions it provides to Grepr regarding the processing of such Personal Data. Customer shall not provide or make available to Grepr any Personal Data in violation of the Agreement or otherwise inappropriate for the nature of the Services, and shall indemnify Grepr from all claims and losses in connection therewith.

2.2 Grepr shall not process Personal Data (i) for purposes other than those set forth in the Agreement and/or Exhibit A, (ii) in a manner inconsistent with the terms and conditions set forth in this DPA or any other documented instructions provided by Customer, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Supervisory Authority to which the Grepr is subject; in such a case, the Grepr shall inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest, or (iii) in violation of Data Protection Laws. Customer hereby instructs Grepr to process Personal Data in accordance with the foregoing and as part of any processing initiated by Customer in its use of the Services.

2.3 The subject matter, nature, purpose, and duration of this processing, as well as the types of Personal Data collected and categories of Data Subjects, are described in Exhibit A to this DPA.

2.4 Following completion of the Services, at Customer's choice, Grepr shall return or delete Customer's Personal Data, unless further storage of such Personal Data is required or authorized by applicable law. If return or destruction is impracticable or prohibited by law, rule or regulation, Grepr shall take measures to block such Personal Data from any further processing (except to the extent necessary for its continued hosting or processing required by law, rule or regulation) and shall continue to appropriately protect the Personal Data remaining in its possession, custody, or control. If Customer and Grepr have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), the parties agree that the certification of deletion of Personal Data that is described in Clause 8.1(d) and Clause 8.5 of the EU SCCs (as applicable) shall be provided by Grepr to Customer only upon Customer's request.

2.5 U.S. State Privacy Law Language. The Parties acknowledge and agree that the processing of personal information or personal data that is subject to the CCPA, VCDPA, CPA, CTDPA, UCPA, or MHMDA shall be carried out in accordance with the terms set forth in Exhibit E.

3. Confidentiality

Grepr shall ensure that any person it authorizes to process Personal Data has agreed to protect Personal Data in accordance with Grepr's confidentiality obligations in the Agreement. Customer agrees that Grepr may disclose Personal Data to its advisers, auditors or other third parties as reasonably required in connection with the performance of its obligations under this DPA, the Agreement, or the provision of Services to Customer.

4. Authorized Subprocessors

4.1 Customer acknowledges and agrees that Grepr may (1) engage its Affiliates and the Authorized Subprocessors listed in Exhibit B to this DPA to access and process Personal Data in connection with the Services and (2) from time to time engage additional third parties for the purpose of providing the Services, including

without limitation the processing of Personal Data. By way of this DPA, Customer provides general written authorization to Grepr to engage subprocessors as necessary to perform the Services.

4.2 A list of Grepr's current Authorized Subprocessors (the "List") will be made available to Customer, either attached hereto, at a link provided to Customer, via email or through another means made available to Customer. Such List may be updated by Grepr from time to time. Grepr may provide a mechanism to subscribe to notifications of new Authorized Subprocessors and Customer agrees to subscribe to such notifications where available. At least ten (10) days before enabling any third party other than existing Authorized Subprocessors to access or participate in the processing of Personal Data, Grepr will add such third party to the List and notify Customer via email. Customer may object to such an engagement by informing Grepr within ten (10) days of receipt of the aforementioned notice to Customer, provided such objection is in writing and based on reasonable grounds relating to data protection. Customer acknowledges that certain subprocessors are essential to providing the Services and that objecting to the use of a subprocessor may prevent Grepr from offering the Services to Customer.

4.3 If Customer reasonably objects to an engagement in accordance with Section 4.2, and Grepr cannot provide a commercially reasonable alternative within a reasonable period of time, Customer may discontinue the use of the affected Service by providing written notice to Grepr. Discontinuation shall not relieve Customer of any fees owed to Grepr under the Agreement.

4.4 If Customer does not object to the engagement of a third party in accordance with Section 4.2 within ten (10) days of notice by Grepr, that third party will be deemed an Authorized Subprocessor for the purposes of this DPA.

4.5 Grepr will enter into a written agreement with the Authorized Subprocessor imposing on the Authorized Subprocessor data protection obligations comparable to those imposed on Grepr under this DPA with respect to the protection of Personal Data. In case an Authorized Subprocessor fails to fulfill its data protection obligations under such written agreement with Grepr, Grepr will remain liable to Customer for the performance of the Authorized Subprocessor's obligations under such agreement.

4.6 If Customer and Grepr have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), (i) the above authorizations will constitute Customer's prior written consent to the subcontracting by Grepr of the processing of Personal Data if such consent is required under the Standard Contractual Clauses, and (ii) the parties agree that the copies of the agreements with Authorized Subprocessors that must be provided by Grepr to Customer pursuant to Clause 9(c) of the EU SCCs may have commercial information, or information unrelated to the Standard Contractual Clauses or their equivalent, removed by the Grepr beforehand, and that such copies will be provided by the Grepr only upon request by Customer.

5. Security of Personal Data.

Taking into account 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, Grepr shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of processing Personal Data. Exhibit C sets forth additional information about Grepr's technical and organizational security measures.

6. Transfers of Personal Data

6.1 The parties agree that Grepr may transfer Personal Data processed under this DPA outside the EEA, the UK, or Switzerland as necessary to provide the Services. Where Customer has been provisioned on a Grepr service region located within the EEA, Grepr will store and process Personal Data at rest within the EEA and will not store Personal Data at rest outside the EEA except as expressly agreed in writing by Customer. Customer acknowledges that Grepr personnel and Authorized Subprocessors located outside the EEA, including in the United States, may access Personal Data remotely for the purposes of providing, maintaining, monitoring, securing, and supporting the Services, including incident response, troubleshooting, and technical support. Such access constitutes an ex-EEA Transfer and is subject to this Section 6 and to the technical and organizational measures set forth in Exhibit C. If Grepr transfers Personal Data protected under this DPA to a jurisdiction for which the European Commission has not issued an adequacy decision, Grepr will ensure that appropriate safeguards have been implemented for the transfer of Personal Data in accordance with Data Protection Laws.

6.2 Ex-EEA Transfers. The parties agree that ex-EEA Transfers will be made (i) for so long as Grepr maintains an active certification under the Data Privacy Framework and the relevant adequacy decision remains in force, pursuant to the Data Privacy Framework, or (ii) at all other times, pursuant to the EU SCCs, which are deemed entered into (and incorporated into this DPA by this reference), which take effect automatically and without further action by either party whenever subsection (i) does not apply, and which are completed as follows:

6.2.1 Module One (Controller to Controller) of the EU SCCs apply when Grepr is processing Personal Data as a controller pursuant to Section 9 of this DPA.

6.2.2 Module Two (Controller to Processor) of the EU SCCs apply when Customer is a controller and Grepr is processing Personal Data for Customer as a processor pursuant to Section 2 of this DPA.

6.2.3 Module Three (Processor to Subprocessor) of the EU SCCs apply when Customer is a processor and Grepr is processing Personal Data on behalf of Customer as a subprocessor.

6.2.4 Module Four (Processor to Controller) of the EU SCCs apply when Customer is a processor of Grepr Usage Data and Grepr processes Grepr Usage Data as a controller.

6.3 For each module, where applicable the following applies:

6.3.1 In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of subprocessor changes shall be as set forth in Section 4.2 of this DPA;

6.3.2 All square brackets in Clause 13 are hereby removed;

6.3.3 In Clause 17 (Option 1), the EU SCCs will be governed by Irish law;

6.3.4 In Clause 18(b), disputes will be resolved before the courts of Dublin;

6.3.5 Exhibit B to this DPA contains the information required in Annex I and Annex III of the EU SCCs;

6.3.6 Exhibit C to this DPA contains the information required in Annex II of the EU SCCs; and

6.3.7 By entering into this DPA, the parties are deemed to have signed the EU SCCs incorporated herein, including their Annexes.

6.4 Ex-UK Transfers. The parties agree that ex-UK Transfers will be made (i) pursuant to the Data Privacy Framework, or (ii) if the Data Privacy Framework does not apply or ceases to be available, pursuant to the UK SCCs, which are deemed entered into and incorporated into this DPA by reference, and amended and completed in accordance with the UK Addendum, which is incorporated herein as Exhibit D of this DPA. Subsection (i) of this Section 6.4 applies only for so long as Grepr maintains an active certification under the UK Extension to the EU-U.S. Data Privacy Framework and the relevant adequacy regulations remain in force; at all other times, ex-UK Transfers will be made pursuant to the UK SCCs, which take effect automatically and without further action by either party.

6.5 Transfers from Switzerland. The parties agree that transfers from Switzerland will be made (i) for so long as Grepr maintains an active certification under the Swiss-U.S. Data Privacy Framework and the relevant adequacy decision remains in force, pursuant to the Data Privacy Framework, or (ii) at all other times, pursuant to the EU SCCs with the following modifications:

6.5.1 The terms "General Data Protection Regulation" or "Regulation (EU) 2016/679" as utilized in the EU SCCs shall be interpreted to include the Federal Act on Data Protection of 19 June 1992 (the "FADP," and as revised as of 25 September 2020, the "Revised FADP") with respect to data transfers subject to the FADP.

6.5.2

6.5.3 Clause 13 of the EU SCCs is modified to provide that the Federal Data Protection and Information Commissioner ("FDPIC") of Switzerland shall have authority over data transfers governed by the FADP and the appropriate EU supervisory authority shall have authority over data transfers governed by the GDPR. Subject to the foregoing, all other requirements of Clause 13 shall be observed.

6.5.4 The term "EU Member State" as utilized in the EU SCCs shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from exercising their rights in their place of habitual residence in accordance with Clause 18(c) of the EU SCCs.

6.6 Supplementary Measures. In respect of any ex-EEA Transfer or ex-UK Transfer made pursuant to the Standard Contractual Clauses, the following supplementary measures shall apply:

6.6.1 As of the date of this DPA, the Data Importer has not received any formal legal requests from any government intelligence or security service/agencies in the country to which the Personal Data is being exported, for access to (or for copies of) Customer's Personal Data ("Government Agency Requests");

6.6.2 If, after the date of this DPA, the Data Importer receives any Government Agency Requests, Grepr shall attempt to redirect the law enforcement or government agency to request that data directly from Customer. As part of this effort, Grepr may provide Customer's basic contact information to the government agency. If compelled to disclose Customer's Personal Data to a law enforcement or government agency, Grepr shall give Customer reasonable notice of the demand and cooperate to allow Customer to seek a protective order or other appropriate remedy unless Grepr is legally prohibited from doing so. Grepr shall not voluntarily disclose Personal Data to any law enforcement or government agency. Data Exporter and Data Importer shall (as soon as reasonably practicable) discuss and determine whether all or any transfers of Personal Data pursuant to this DPA should be suspended in the light of the such Government Agency Requests;

6.6.3 The Data Exporter and Data Importer will meet regularly to consider whether:

(i) the protection afforded by the laws of the country of the Data Importer to data subjects whose Personal Data is being transferred is sufficient to provide broadly equivalent protection to that afforded in the EEA or the UK, whichever the case may be;

(ii) additional measures are reasonably necessary to enable the transfer to be compliant with the Data Protection Laws; and

(iii) it is still appropriate for Personal Data to be transferred to the relevant Data Importer, taking into account all relevant information available to the parties, together with guidance provided by the supervisory authorities.

6.6.4 If Data Protection Laws require the Data Exporter to execute the Standard Contractual Clauses applicable to a particular transfer of Personal Data to a Data Importer as a separate agreement, the Data Importer shall, on request of the Data Exporter, promptly execute such Standard Contractual Clauses incorporating such amendments as may reasonably be required by the Data Exporter to reflect the applicable appendices and annexes, the details of the transfer and the requirements of the relevant Data Protection Laws.

6.6.5 If either (i) any of the means of legitimizing transfers of Personal Data outside of the EEA or UK set forth in this DPA cease to be valid or (ii) any supervisory authority requires transfers of Personal Data pursuant to those means to be suspended, then Data Importer may by notice to the Data Exporter, with effect from the date set out in such notice, amend or put in place alternative arrangements in respect of such transfers, as required by Data Protection Laws.

7. Rights of Data Subjects

7.1 Grepr shall, to the extent permitted by law, notify Customer upon receipt of a request by a Data Subject to exercise the Data Subject's right of: access, rectification, erasure, data portability, restriction or cessation of processing, withdrawal of consent to processing, and/or objection to being subject to processing that constitutes automated decision-making (such requests individually and collectively "Data Subject Request(s)"). If Grepr receives a Data Subject Request in relation to Customer's data, Grepr will advise the Data Subject to submit their request to Customer and Customer will be responsible for responding to such request, including, where necessary, by using the functionality of the Services. Customer is solely responsible for ensuring that Data Subject Requests for erasure, restriction or cessation of processing, or withdrawal of consent to processing of any Personal Data are communicated to Grepr, and, if applicable, for ensuring that a record of consent to processing is maintained with respect to each Data Subject.

7.2 Grepr shall, at the request of the Customer, and taking into account the nature of the processing applicable to any Data Subject Request, apply appropriate technical and organizational measures to assist Customer in complying with Customer's obligation to respond to such Data Subject Request and/or in demonstrating such compliance, where possible, *provided that* (i) Customer is itself unable to respond without Grepr's assistance and (ii) Grepr is able to do so in accordance with all applicable laws, rules, and regulations. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Grepr.

8. Actions and Access Requests; Audits

8.1 Grepr shall, taking into account the nature of the processing and the information available to Grepr, provide Customer with reasonable cooperation and assistance where necessary for Customer to comply with its obligations under the Data Protection Laws to conduct a data protection impact assessment and/or to

demonstrate such compliance, *provided that* Customer does not otherwise have access to the relevant information. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Grepr.

8.2 Grepr shall, taking into account the nature of the processing and the information available to Grepr, provide Customer with reasonable cooperation and assistance with respect to Customer's cooperation and/or prior consultation with any Supervisory Authority or regulatory agency, where necessary and where required by the Data Protection Laws. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Grepr.

8.3 Grepr shall maintain records sufficient to demonstrate its compliance with its obligations under this DPA, and retain such records for a period of three (3) years after the termination of the Agreement. Customer shall, with reasonable notice to Grepr, have the right to review, audit and copy such records at Grepr's offices during regular business hours.

8.4 Upon Customer's written request at reasonable intervals, and subject to reasonable confidentiality controls, Grepr shall, either (i) make available for Customer's review copies of such certifications or reports, if any, as Grepr then maintains demonstrating Grepr's compliance with prevailing data security standards applicable to the processing of Customer's Personal Data, or (ii) if the provision of reports or certifications pursuant to (i) is not reasonably sufficient under Data Protection Laws, allow Customer's independent third party representative to conduct an audit or inspection of Grepr's data security infrastructure and procedures that is sufficient to demonstrate Grepr's compliance with its obligations under Data Protection Laws, provided that (a) Customer provides reasonable prior written notice of any such request for an audit and such inspection shall not be unreasonably disruptive to Grepr's business; (b) such audit shall only be performed during business hours and occur no more than once per calendar year; and (c) such audit shall be restricted to data relevant to Customer. Customer shall be responsible for the costs of any such audits or inspections, including without limitation a reimbursement to Grepr for any time expended for on-site audits. If Customer and Grepr have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), the parties agree that the audits described in Clause 8.9 of the EU SCCs shall be carried out in accordance with this Section 8.4.

8.5 Grepr shall immediately notify Customer if an instruction, in the Grepr's opinion, infringes the Data Protection Laws or Supervisory Authority.

8.6 In the event of a Personal Data Breach, Grepr shall, without undue delay, inform Customer of the Personal Data Breach and take such steps as Grepr in its sole discretion deems necessary and reasonable to remediate such violation (to the extent that remediation is within Grepr's reasonable control).

8.7 In the event of a Personal Data Breach, Grepr shall, taking into account the nature of the processing and the information available to Grepr, provide Customer with reasonable cooperation and assistance necessary for Customer to comply with its obligations under the Data Protection Laws with respect to notifying (i) the relevant Supervisory Authority or regulatory agency and (ii) Data Subjects affected by such Personal Data Breach without undue delay.

8.8 The obligations described in Sections 8.6 and 8.7 shall not apply in the event that a Personal Data Breach results from the actions or omissions of Customer. Grepr's obligation to report or respond to a Personal Data Breach under Sections 8.6 and 8.7 will not be construed as an acknowledgement by Grepr of any fault or liability with respect to the Personal Data Breach.

9. Grepr's Role as a Controller. The parties acknowledge and agree that with respect to Grepr Account Data and Grepr Usage Data, Grepr is an independent controller, not a joint controller with Customer. Grepr will process Grepr Account Data and Grepr Usage Data as a controller (i) to manage the relationship with Customer; (ii) to carry out Grepr's core business operations, such as accounting, audits, tax preparation and filing and compliance purposes; (iii) to monitor, investigate, prevent and detect fraud, security incidents and other misuse of the Services, and to prevent harm to Customer; (iv) for identity verification purposes; (v) to comply with legal or regulatory obligations applicable to the processing and retention of Personal Data to which Grepr is subject; and (vi) as otherwise permitted under Data Protection Laws and in accordance with this DPA and the Agreement. Grepr may also process Grepr Usage Data as a controller to provide, optimize, and maintain the Services, to the extent permitted by Data Protection Laws.

10. Conflict. In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) the applicable terms in the Standard Contractual Clauses; (2) the terms of this DPA; (3) the Agreement; and (4) the Grepr's privacy policy. Any claims brought in connection with this DPA will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations set forth in the Agreement.

Exhibit A

Details of Processing

Nature and Purpose of Processing: Grepr will process Customer's Personal Data as necessary to provide the Services under the Agreement and for the purposes specified in the Agreement and this DPA. The nature of processing includes, without limitation:

Receiving data, including collection, accessing, retrieval, recording, and data entry
Holding data, including storage, organization and structuring
Using data, including analysis, consultation, testing, automated decision making and profiling
Updating data, including correcting, adaptation, alteration, alignment and combination
Protecting data, including restricting, encrypting, and security testing
Sharing data, including disclosure, dissemination, allowing access or otherwise making available
Returning data to the data exporter or data subject
Erasing data, including destruction and deletion

Duration of Processing: Grepr will process Customer's Personal Data as long as required (i) to provide the Services to Customer under the Agreement; (ii) for Grepr's legitimate business needs; or (iii) by applicable law or regulation.

Categories of Data Subjects: (i) employees, contractors, and agents of Customer whom Customer authorizes to access the Services; (ii) individuals at Customer with whom Grepr maintains a commercial, billing, or support relationship, and (iii) any other individuals whose data Customer provides or makes available.

Categories of Personal Data: Grepr processes any Personal Data provided or made available by Customer (including any Personal Data Customer collects from its end users and processes through its use of the Services) or collected by Grepr in order to provide the Services or as otherwise set forth in the Agreement or this DPA.

Sensitive Data or Special Categories of Data: Customer is responsible for scrubbing sensitive data before sending to Grepr for processing.

Exhibit B

The following includes the information required by Annex I and Annex III of the EU SCCs, and Table 1, Annex 1A, and Annex 1B of the UK Addendum.

1. **The Parties**

   Data exporter(s): The Customer

   Contact details: As designated by Customer's account or in an Order

   Signature and date: By entering into the Agreement, Data Exporter is deemed to have signed these Standard Contractual Clauses incorporated herein, as of the Effective Date of the Agreement.

   Role (controller/processor): The Data Exporter's role is set forth in Section 2 of this Addendum.

   Data importer(s): Grepr, Inc.

   Address: As specified in the Agreement

   Contact person's name, position and contact details: Jad Naous, CEO, legalnotices@grepr.ai

   Signature and date: By entering into the Agreement, Data Importer is deemed to have signed these Standard Contractual Clauses incorporated herein, as of the Effective Date of the Agreement.

   Role (controller/processor): The Data Importer's role is set forth in Section 2 of this Addendum.

2. Description of the Transfer

Data Subjects	As described in Exhibit A of the DPA
Categories of Personal Data	As described in Exhibit A of the DPA
Special Category Personal Data (if applicable)	As described in Exhibit A of the DPA
Nature of the Processing	As described in Exhibit A of the DPA
Purposes of Processing	As described in Exhibit A of the DPA
Duration of Processing and Retention (or the criteria to determine such period)	As described in Exhibit A of the DPA
Frequency of the transfer	As necessary to provide perform all obligations and rights with respect to Personal Data as provided in the Agreement or DPA
Recipients of Personal Data Transferred to the Data Importer	Grepr's list of Subprocessors can be found below

3. Competent Supervisory Authority

The supervisory authority shall be the supervisory authority of the Data Exporter, as determined in accordance with Clause 13 of the EU SCCs. The supervisory authority for the purposes of the UK Addendum shall be the UK Information Commissioner's Officer.

4. List of Authorized Subprocessors

Name of Authorized Subprocessor	**Description of processing**	**Country in which subprocessing will take place**
Amazon AWS	Provides application infrastructure	USA
Datadog	Provides performance monitoring	USA
Auth0	Provides authentication and authorization services	USA
Google	Storage and processing of documents related to the business	USA
Intercom	Ticketing and customer support	USA
Slack	Messaging and Communications	USA
Hubspot	CRM system	USA
Salesbricks	Metering and invoicing	USA
Notion	Wiki and internal project management	USA
PagerDuty	Incident management and notifications	USA

Exhibit C

Description of the Technical and Organisational Security Measures implemented by the Data Importer

The following includes the information required by Annex II of the EU SCCs and Annex II of the UK Addendum.

Technical and Organizational Security Measure	**Details**
Measures of pseudonymisation and encryption of personal data	Data is encrypted in transit and at rest using industry-standard encryption. Data processed through Grepr's pipeline and stored in Grepr's storage may contain Data, the categories of which are determined solely by Customer, as described in Exhibit A. Grepr Account Data, including email addresses of individuals authorized by Customer to access the Services, is stored with a third-party service provider that maintains ISO 27018 data encryption standards.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Grepr's uses processes and tools to create, assign, manage, and revoke access credentials and privileges for users, and administrators systems. Greper has processes and technical controls to identify, classify, securely handle, retain, and dispose of data, as defined in this document. Greper's data recovery practices follow industry standards, and detail is provided in this document regarding maintenance of raw data.
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	All original data logs are maintained in Grepr, which means all data is available in the case of a physical or technical incident. Grepr maintains backup and disaster-recovery copies on a rolling seven (7) day cycle, which are accessed or restored only for disaster-recovery purposes or as required by applicable law.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	Grepr practices unit testing and reviews the outcomes of each test in development before migrating any code to production. Security testing is performed by a PCI Qualified Security Assessor Company. They perform pentesting on the Grepr API to ensure data protection. Vulnerabilities are reported to Grepr, and they are addressed prior to re-testing. This process occurs until vulnerabilities are clear.
Measures for user identification and authorization	Grepr conducts regular access reviews for the in-scope system components to help ensure that access is restricted.
Measures for the protection of data during transmission	During transmission, web servers use secure HTTPS protocol to communicate with websites, which uses TLS encryption methods. They authenticate both communicating parties.
Measures for the protection of data during storage	Data is encrypted at rest in Grepr's storage using industry-standard encryption. Multi-tenant services have access to all of their data, and have permissions to r/w all data. Writing data only is possible for the Customer's individual bucket. Single tenant services only have permissions to r/w for that customer.
Measures for ensuring physical security of locations at which personal data are processed	Grepr has multiple physical security measures in place, including a gate with authentication, two physical locks, a main door office lock, and a building security alarm.
Measures for ensuring events logging	All logs are processed by Grepr, and then stored in S3 or other highly-durable storage. This ensures that a copy of logs exists for troubleshooting and auditing. Grepr uses log aggregation tools to have access to recent logs.
Measures for ensuring system configuration,	All Grepr settings are deployed in a standard format. If a Customer requests a non-standard feature, Grepr will investigate the feasibility and impact of enabling the feature, and then discuss with the Customer. If it's

including default configuration	acceptable, Grepr will deploy configuration modifications for only that Customer.
Measures for internal IT and IT security governance and management	All Grepr staff are required to install security monitoring software on their machines, encrypt their harddrive, install and use password management software, and take security training on a regular basis. This is monitored by a third-party security monitoring service that maintains SOC 2 Type II and ISO 27001 compliance certification. The outputs are reviewed by leadership. A third-party provider with accreditation in ISO 27001, ISO 27701, and ISO 22301 tests Grepr's API for customer data protection using pen testing. Any vulnerabilities are reported to Grepr. Any detected vulnerabilities that require remediation will be addressed and resolved by Grepr, and then re-tested until clear.
Measures for certification/assurance of processes and products	Grepr uses accredited third-party service providers to audit and maintain SOC 2. Grepr's SOC 2 audit is conducted by the third-party provider. To ensure objectability, evidence to perform the audit is collected by a separate third-party provider. The audits occur on a frequency that is necessary to maintain high quality business and operational standards.
Measures for ensuring data minimisation	Grepr only collects absolutely required information for use.
Measures for ensuring data quality	Grepr does not evaluate the quality of the data provided by the Customer. When data is received from the Customer, a copy of the raw data is made in case it is needed for reprocessing or other reasons. Grepr uses standard data processing systems that are widely used and tested against industry standards. Grepr's data management process and selected processing systems ensure that data quality remains the same as the Customer's originally provided data.
Measures for ensuring limited data retention	Any data stored by Grepr on behalf of the customer is deleted on request. All backup mechanisms have limited retention.
Measures for ensuring accountability	There are multiple steps to ensure accountability at Grepr. Before an employee or staff member begins work at Grepr, a clear background check is required. Prior to granting access to systems and documentation, the employee or staff member is required to complete onboarding training that includes reviewing company policies, accepting said policies, performing security training, and installing device monitoring. These requirements are actively monitored by a third party service provider, Vanta.
Measures for allowing data portability and ensuring erasure	All Grepr employees and staff are required to install and use password management software, which ensures data portability. We use SSO. All data is stored in the cloud, which protects portability. In case data erasure is required, Grepr needs to be informed by the Customer and the erasing process will be completed.
Technical and organizational measures of subprocessors	Grepr enters into Data Processing Agreements with its Authorized Subprocessors with data protection obligations substantially similar to those contained in this DPA.

Exhibit D

UK Addendum

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

Part 1: Tables

Table 1: Parties

Start Date	This UK Addendum shall have the same effective date as the DPA	
The Parties	Exporter	Importer
Parties' Details	Customer	Grepr
Key Contact	*See* Exhibit B of this DPA	*See* Exhibit B of this DPA

Table 2: Selected SCCs, Modules and Selected Clauses

EU SCCs	The Version of the Approved EU SCCs which this UK Addendum is appended to as defined in the DPA and completed by Section 6.2 and 6.3 of the DPA.

Table 3: Appendix Information

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

Annex 1A: List of Parties	As per Table 1 above
Annex 2B: Description of Transfer	*See* Exhibit B of this DPA
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:	*See* Exhibit C of this DPA
Annex III: List of Sub processors (Modules 2 and 3 only):	*See* Exhibit B of this DPA

Table 4: Ending this UK Addendum when the Approved UK Addendum Changes

Ending this UK Addendum when the Approved UK Addendum changes	☒ Importer ☐ Exporter ☐ Neither Party

Entering into this UK Addendum:

1. Each party agrees to be bound by the terms and conditions set out in this UK Addendum, in exchange for the other party also agreeing to be bound by this UK Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making ex-UK Transfers, the Parties may enter into this UK Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this UK Addendum. Entering into this UK Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this UK Addendum

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

UK Addendum	means this International Data Transfer Addendum incorporating the EU SCCs, attached to the DPA as Exhibit D.
EU SCCs	means the version(s) of the Approved EU SCCs which this UK Addendum is appended to, as set out in Table 2, including the Appendix Information
Appendix Information	shall be as set out in Table 3
Appropriate Safeguards	means the standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making an ex-UK Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved UK Addendum	means the template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as may be revised under Section 19 of the UK Addendum.
Approved EU SCCs	means the standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021, for transfers of personal data to countries not otherwise recognized as offering an adequate level of protection for personal data by the European Commission (as amended and updated from time to time).
ICO	means the Information Commissioner of the United Kingdom.
ex-UK Transfer	shall have the same definition as set forth in the DPA .
UK	means the United Kingdom of Great Britain and Northern Ireland
UK Data Protection Laws	means all laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	shall have the definition set forth in the DPA.

4. The UK Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the UK Addendum amend the Approved EU SCCs in any way which is not permitted under the Approved EU SCCs or the Approved UK Addendum, such amendment(s) will not be incorporated in the UK Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and the UK Addendum, UK Data Protection Laws applies.

7. If the meaning of the UK Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after the UK Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for ex-UK Transfers, the hierarchy in Section 10 below will prevail.

10. Where there is any inconsistency or conflict between the Approved UK Addendum and the EU SCCs (as applicable), the Approved UK Addendum overrides the EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved UK Addendum.

11. Where this UK Addendum incorporates EU SCCs which have been entered into to protect ex-EU Transfers subject to the GDPR, then the parties acknowledge that nothing in the UK Addendum impacts those EU SCCs.

Incorporation and Changes to the EU SCCs:

12. This UK Addendum incorporates the EU SCCs which are amended to the extent necessary so that:

    a) together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b) Sections 9 to 11 above override Clause 5 (Hierarchy) of the EU SCCs; and

13. the UK Addendum (including the EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales.

14. Unless the parties have agreed alternative amendments which meet the requirements of Section 12 of this UK Addendum, the provisions of Section 15 of this UK Addendum will apply.

15. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 of this UK Addendum may be made.

16. The following amendments to the EU SCCs (for the purpose of Section 12 of this UK Addendum) are made:

    a) References to the "Clauses" means this UK Addendum, incorporating the EU SCCs;

    b) In Clause 2, delete the words: "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",

    c) Clause 6 (Description of the transfer(s)) is replaced with: "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

    d) Clause 8.7(i) of Module 1 is replaced with: "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

    e) Clause 8.8(i) of Modules 2 and 3 is replaced with: "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

    f) References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

    g) References to Regulation (EU) 2018/1725 are removed;

    h) References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i) The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j) Clause 13(a) and Part C of Annex I are not used;

k) The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l) In Clause 16(e), subsection (i) is replaced with: "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m) Clause 17 is replaced with: "These Clauses are governed by the laws of England and Wales.";

n) Clause 18 is replaced with: "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The parties agree to submit themselves to the jurisdiction of such courts."; and

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

Amendments to the UK Addendum

17. The parties may agree to change Clauses 17 and/or 18 of the EU SCCs to refer to the laws and/or courts of Scotland and Northern Ireland.

18. If the parties wish to change the format of the information included in Part 1: Tables of the Approved UK Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

19. From time to time, the ICO may issue a revised Approved UK Addendum which:

    a) makes reasonable and proportionate changes to the Approved UK Addendum, including correcting errors in the Approved UK Addendum; and/or

    b) reflects changes to UK Data Protection Laws;

    The revised Approved UK Addendum will specify the start date from which the changes to the Approved UK Addendum are effective and whether the parties need to review this UK Addendum including the Appendix Information. This UK Addendum is automatically amended as set out in the revised Approved UK Addendum from the start date specified.

20. If the ICO issues a revised Approved UK Addendum under Section 18 of this UK Addendum, if a party will as a direct result of the changes in the Approved UK Addendum have a substantial, disproportionate and demonstrable increase in:

    c) its direct costs of performing its obligations under the UK Addendum; and/or

    d) its risk under the UK Addendum,

    and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that party may end this UK Addendum at the end of a reasonable notice period, by providing written notice for that period to the other party before the start date of the revised Approved UK Addendum.

21. The parties do not need the consent of any third party to make changes to this UK Addendum, but any changes must be made in accordance with its terms.

Exhibit E

United States Privacy Law Exhibit

This United States Privacy Law Exhibit ("Exhibit") supplements the DPA and includes additional information required by the CCPA, the VCDPA, the CPA, the CTDPA, the UCPA, and the MHMDA in each case, as updated, amended or replaced from time to time. Any terms not defined in this Exhibit shall have the meanings set forth in the DPA and/or the Agreement.

A. CALIFORNIA

1. Definitions

1.1 For purposes of this Section A, the terms "Business," "Business Purpose," "Commercial Purpose," "Consumer," "Personal Information," "Processing," "Sell," "Service Provider," "Share," and "Verifiable Consumer Request" shall have the meanings set forth in the CCPA.

1.2 All references to "Personal Data," "Controller," "Processor," and "Data Subject" in the DPA shall be deemed to be references to "Personal Information," "Business," "Service Provider," and "Consumer," respectively, as defined in the CCPA.

2. Obligations

2.1 Except with respect to Grepr Account Data and Grepr Usage Data (as defined in the DPA), the parties acknowledge and agree that Grepr is a Service Provider for the purposes of the CCPA (to the extent it applies) and Grepr is receiving Personal Information from Customer in order to provide the Services pursuant to the Agreement, which constitutes a Business Purpose.

2.2 Customer shall disclose Personal Information to Grepr only for the limited and specified purposes described in Exhibit A to this DPA.

2.3 Grepr shall not Sell or Share Personal Information provided by Customer under the Agreement.

2.4 Grepr shall not retain, use, or disclose Personal Information provided by Customer pursuant to the Agreement for any purpose, including a Commercial Purpose, other than as necessary for the specific purpose of performing the Services for Customer pursuant to the Agreement, or as otherwise set forth in the Agreement or as permitted by the CCPA.

2.5 Grepr shall not retain, use, or disclose Personal Information provided by Customer pursuant to the Agreement outside of the direct business relationship between Grepr and Customer, except where and to the extent permitted by the CCPA.

2.6 Grepr shall notify Customer if it makes a determination that it can no longer meet its obligations under the CCPA.

2.7 Grepr will not combine Personal Information received from, or on behalf of, Customer with Personal Information that it receives from, or on behalf of, another party, or that it collects from its own interaction with the Consumer.

2.8 Grepr shall comply with all obligations applicable to Service Providers under the CCPA, including by providing Personal Information provided by Customer under the Agreement the level of privacy protection required by CCPA.

2.9 Grepr shall only engage a new subprocessor to assist Grepr in providing the Services to Customer under the Agreement in accordance with Section 4.1 of the DPA, including, without limitation, by: (i) notifying Customer of such engagement via the notification mechanism described in Section 4.1 of the DPA at least ten (10) days before enabling a new Subprocessor; and (ii) entering into a written contract with the subprocessor requiring subprocessor to observe all of the applicable requirements set forth in the CCPA.

3. Consumer Rights

3.1 Grepr shall assist Customer in responding to Verifiable Consumer Requests to exercise the Consumer's rights under the CCPA as set forth in Section 7 of the DPA.

4. Audit and Remediation Rights

4.1 To the extent required by CCPA, Grepr shall allow Customer to conduct inspections or audits in accordance with Sections 8.3 and 8.4 of the DPA.

4.2 If Customer determines that Grepr is Processing Personal Information in an unauthorized manner, Customer may, taking into account the nature of the Grepr's Processing and the nature of the Personal Information Processed by Grepr on

behalf of Customer, take commercially reasonable and appropriate steps to stop and remediate such unauthorized Processing.

B. VIRGINIA

1. Definitions

1.1 For purposes of this Section B, the terms "Consumer," "Controller," "Personal Data," "Processing," and "Processor" shall have the meanings set forth in the VCDPA.

1.2 All references to "Data Subject" in this DPA shall be deemed to be references to "Consumer" as defined in the VCDPA.

2. Obligations

2.1 Except with respect to Grepr Account Data and Grepr Usage Data (as defined in the DPA), the parties acknowledge and agree that Customer is a Controller and Grepr is a Processor for the purposes of the VCDPA (to extent it applies).

2.2 The nature, purpose, and duration of Processing, as well as the types of Personal Data and categories of Consumers are described in Exhibit A to this DPA.

2.3 Grepr shall adhere to Customer's instructions with respect to the Processing of Customer Personal Data and shall assist Customer in meeting its obligations under the VCDPA by:

2.3.1 Assisting Customer in responding to Consumer rights requests under the VCDPA as set forth in Section 7 of the DPA;

2.3.2 Complying with Section 5 ("Security of Personal Data") of the DPA with respect to Personal Data provided by Customer;

2.3.3 In the event of a Personal Data Breach, providing information sufficient to enable Customer to meet its obligations pursuant to Virginia's breach notification laws (Va. Code § 18.2-186.6); and

2.3.4 Providing information sufficient to enable Customer to conduct and document data protection assessments to the extent required by VCDPA.

2.4 Grepr shall maintain the confidentiality of Personal Data provided by Customer and require that each person Processing such Personal Data be subject to a duty of confidentiality with respect to such Processing.

2.5 Upon Customer's written request, Grepr shall delete or return all Personal Data provided by Customer in accordance with Section 2.4 of the DPA, unless retention of such Personal Data is required or authorized by law or the DPA and/or Agreement.

2.6 In the event that Grepr engages a new subprocessor to assist Grepr in providing the Services to Customer under the Agreement, Grepr shall enter into a written contract with the subprocessor requiring subprocessor to observe all of the applicable requirements of a Processor set forth in the VCDPA.

3. Audit Rights

3.1 Upon Customer's written request at reasonable intervals, Grepr shall, as set forth in Sections 8.3-8.4 of the DPA, (i) make available to Customer all information in its possession that is reasonably necessary to demonstrate Grepr's compliance with its obligations under the VCDPA; and (ii) allow and cooperate with reasonable inspections or audits as required under the VCDPA.

C. COLORADO

1. Definitions

1.1 For purposes of this Section C, the terms "Consumer," "Controller," "Personal Data," "Processing," and "Processor" shall have the meanings set forth in the CPA.

1.2 All references to "Data Subject" in the DPA shall be deemed to be references to "Consumer" as defined in the CPA.

2. Obligations

2.1 Except with respect to Grepr Account Data and Grepr Usage Data (as defined in the DPA), the parties acknowledge and agree that Customer is a Controller and Grepr is a Processor for the purposes of the CPA (to extent it applies).

2.2 The nature, purpose, and duration of Processing, as well as the types of Personal Data and categories of Consumers are described in Exhibit A to this DPA.

2.3 Grepr shall require that each person Processing such Personal Data be subject to a duty of confidentiality with respect to such Processing.

2.4 Grepr shall only engage a new subcontractor to assist Grepr in providing the Services to Customer under the Agreement in accordance with Section 4.1 of the DPA, including, without limitation, by: (i) notifying Customer of such engagement via the notification mechanism described in Section 4.1 of the DPA and providing Customer with an opportunity to object and (ii) entering into a written contract with the subcontractor requiring subcontractor to observe all of the applicable requirements set forth in the CPA.

2.5 Grepr shall be responsible for taking the appropriate technical and organizational measures as described in Exhibit C. Customer shall be responsible for implementing appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

2.6 Upon Customer's written request, Grepr shall delete or return all Personal Data provided by Customer in accordance with Section 2.4 of the DPA, unless retention of such Personal Data is required or authorized by law or the DPA and/or Agreement.

3. Audit Rights

3.1 Upon Customer's written request at reasonable intervals, Grepr shall, as set forth in Sections 8.3-8.4 of the DPA, (i) make available to Customer all information in its possession that is reasonably necessary to demonstrate Grepr's compliance with its obligations under the CPA and (ii) allow and cooperate with reasonable inspections or audits as required or permitted under the CPA.

D. CONNECTICUT

1. Definitions

1.1 For purposes of this Section D, the terms "Consumer," "Controller," "Personal Data," "Processing," and "Processor" shall have the meanings set forth in the CTDPA.

1.2 All references to "Data Subject" in the DPA shall be deemed to be references to "Consumer" as defined in the CTDPA.

2. Obligations

2.1 Except with respect to Grepr Account Data and Grepr Usage Data (as defined in the DPA), the parties acknowledge and agree that Customer is a Controller and Grepr is a Processor for the purposes of the CTDPA (to extent it applies).

2.2 The nature, purpose, and duration of Processing, as well as the types of Personal Data and categories of Consumers are described in Exhibit A to this DPA.

2.3 Grepr shall require that each person Processing such Personal Data be subject to a duty of confidentiality with respect to such Processing.

2.4 Grepr shall only engage a new subcontractor to assist Grepr in providing the Services to Customer under the Agreement in accordance with Section 4.1 of the DPA, including, without limitation, by: (i) notifying Customer of such engagement via the notification mechanism described in Section 4.1 of the DPA and providing Customer with an opportunity to object and (ii) entering into a written contract with the subcontractor requiring subcontractor to observe all of the applicable requirements set forth in the CTDPA.

2.5 Upon Customer's written request, Grepr shall delete or return all Personal Data provided by Customer in accordance with Section 2.4 of the DPA, unless retention of such Personal Data is required or authorized by law or the DPA and/or Agreement.

3. Audit Rights

3.1 Upon Customer's written request at reasonable intervals, Grepr shall, as set forth in Sections 8.3-8.4 of the DPA, (i) make available to Customer all information in its possession that is reasonably necessary to demonstrate Grepr's compliance

with its obligations under the CTDPA and (ii) allow and cooperate with reasonable inspections or audits as required under the CTDPA.

E. UTAH

1. Definitions

1.1 For purposes of this Section E, the terms "Consumer," "Controller," "Personal Data," "Processing," and "Processor" shall have the meanings set forth in the UCPA.

1.2 All references to "Data Subject" in the DPA shall be deemed to be references to "Consumer" as defined in the UCPA.

2. Obligations

2.1 Except with respect to Grepr Account Data and Grepr Usage Data (as defined in the DPA), the parties acknowledge and agree that Customer is a Controller and Grepr is a Processor for the purposes of the UCPA (to extent it applies).

2.2 The instructions with respect to the Processing of Customer Personal Data and the parties' rights and obligations are set forth in this DPA and the Agreement.

2.3 The nature, purpose, and duration of Processing, as well as the types of Personal Data and categories of Consumers are described in Exhibit A to this DPA.

2.4 Grepr shall require that each person Processing such Personal Data be subject to a duty of confidentiality with respect to such Processing.

2.5 Grepr shall only engage a new subcontractor to assist Grepr in providing the Services to Customer under the Agreement in accordance with Section 4.1 of the DPA, including, without limitation, by entering into a written contract with the subcontractor requiring subcontractor to observe all of the applicable requirements set forth in the UCPA.

F. WASHINGTON

1. Definitions

1.1 For purposes of this Section F, the terms "Consumer Health Data," "Processor," "Regulated Entity," "Small Business," and "Process" or "Processing" shall have the meanings set forth in the MHMDA.

1.2 All references to "Data Subject" in the DPA shall be deemed to be references to "Consumer" as defined in the MHMDA.

2. Obligations

2.1 Except with respect to Grepr Account Data and Grepr Usage Data (as defined in the DPA), the parties acknowledge and agree that Grepr is a Processor for the purposes of the MHMDA (to the extent it applies).

2.2 The Customer's instructions with respect to the Grepr's Processing of Consumer Health Data and each party's respective rights and obligations are set forth in this DPA and the Agreement.

2.3 The nature, purpose, and duration of Processing, as well as the types of Consumer Health Data and categories of Consumers are described in Exhibit A to this DPA.

2.4 Grepr shall be responsible for taking the appropriate technical and organizational measures as described in Exhibit C. Customer shall be responsible for implementing appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

2.5 Grepr acknowledges that if it fails to adhere to Customer's instructions or processes Consumer Health Data outside of the scope of the Agreement or this DPA, Grepr may be subject to all the obligations as a Regulated Entity or a Small Business, as applicable, pursuant to the MHMDA.