Docusign Envelope ID: D66DFAE3-4704-8067-813B-BB348A8864F7

Data Processing Agreement

This Data Processing Agreement ("DPA") is between the entity identified below as Customer ("Customer"), and Grafana Labs Inc., with offices at 165 Broadway 23rd Floor, New York, NY 10006 United States of America, on behalf of itself and the Affiliates listed below ("Processor" or "Grafana Labs") and is appended to either: (1) the Grafana Labs Master Services Agreement, (2) an end user license agreement (the online Master Services Agreement, a EULA, clickwrap if any, or clickthrough agreement) accepted by Customer on Customer's initial registration and access of the Grafana Product(s) (the "Services"), or (3) any another written and signed license agreement between the parties under which Processor provides Grafana Product(s) to Customer (as applicable, the "Services Agreement"). This DPA is effective as of the date signed by Customer, but only if Grafana Labs receives the signed DPA in accordance with the instructions below.

This DPA sets forth the terms and conditions under which Processor may receive and process Personal Data from Customer. This DPA takes into account the nature of the processing pursuant to the Services Agreement and describes the appropriate technical and organizational measures undertaken by Processor in the processing of Personal Data.

In addition to Grafana Labs' obligations set out in this DPA, where Customer transfers Personal Data from the EEA, Switzerland and/or the UK to Grafana Labs and to a country that does not ensure an adequate level of protection under the applicable European Data Protection Law, such transfers shall be governed by and performed in accordance with the applicable EU Standard Contractual Clauses and UK International Data Transfer Agreement. Any references therein to **Data Importer** shall be deemed to be a reference to **Grafana Labs Inc., or the Processor,** and any reference to **Data Exporter** or Data Controller shall be deemed to be a reference to **Customer** and its Affiliates. Customer hereby covenants and warrants that it has the right and authority to enter into this DPA on behalf of itself and its affiliated companies.

The Parties to this DPA hereby agree to be bound by the terms and conditions in the attached Schedule 1 (Data Processing Terms), the Appendices thereto, and Schedule 2 (Cross Border Data Transfer Mechanisms). This DPA has been pre-signed by Processor, Grafana Labs Inc. In order for this DPA to be effective, Customer must first:

1. Complete and sign the information block below with Customer full legal entity name, address, and signatory information; and
2. Submit the completed and signed DPA to Grafana Labs via email to legal-ops@grafana.com.

If Customer makes any deletions or other revisions to this DPA, those deletions or revisions are hereby rejected and invalid, unless agreed by Grafana Labs. Customer's signatory represents and warrants that he or she has the legal authority to bind Customer to this DPA. This DPA will terminate automatically upon termination of the Services Agreement, or as earlier terminated pursuant to the terms of this DPA.

Accepted and agreed by **Customer**:	Accepted and agreed by **Grafana Labs:**
Signature:	Signature: Signed by: Lora Blum 4B309F699D084C9...
Name:	Name: Lora Blum
Date:	Chief Legal Officer
Company:	
Address:	

Docusign Envelope ID: D66DFAE3-4704-8067-813B-BB348A8864F7

SCHEDULE 1
DATA PROCESSING TERMS

1. Definitions.

a. All terms used without definition in this DPA have the meanings ascribed to them: first, in the Applicable Data Protection Law; second, as applicable in Schedule 3 (Jurisdiction Specific Terms); and third, in the Services Agreement.

b. **Applicable Data Protection Law** means all laws and regulations regarding the Processing of Personal Data applicable to the provision of Grafana Product(s) under the Services Agreement.

c. **Data Subject** means the identified or identifiable person to whom Personal Data relates.

d. **Personal Data** has the meaning as set forth in Applicable Data Protection Law, as it relates to personal data provided by Customer through the Services.

e. **Subprocessor** means any processor engaged by Grafana Labs to process Personal Data.

2. Processing of Personal Data.

a. It is the intent of the parties that, with respect to the activities described in Appendix 1, Customer and its Affiliates (or their Affiliates or clients) may act either as a controller or processor (data exporter) and Processor will be the data processor / data importer to the extent it processes such Personal Data. Customer agrees and warrants that its instructions to Processor regarding the processing of Personal Data are and shall be in accordance with the relevant provisions of Applicable Data Protection Law.

b. The purpose, subject matter and duration of the Processing of Personal Data are set out in the Services Agreement, which describes the provision of the Services to Customer. The nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects are further set forth in Appendix 1 to this DPA.

c. Customer is responsible for the accuracy, quality, and legality of the Personal Data, and the means by which Customer acquired the Personal Data.

d. The Services Agreement and this DPA hereby form Customer's instructions to Processor regarding: (1) the Processing of Personal Data, and (2) the transfer of such Personal Data to any country or territory, when reasonably necessary for the provision of the Services.

3. Data Protection Impact Assessment; Cooperation with Supervisory Authorities

Taking into account the nature of the Processing, Processor may provide Customer with reasonable cooperation and assistance needed to fulfill Customer's obligation under Applicable Data Protection Law to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Processor. Processor shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this Section 3 of this DPA, to the extent required under Applicable Data Protection Law. Additionally, in connection with the Supervisory Authority's request, at Customer's expense, Processor shall make reasonable efforts to acquire the reasonable cooperation and assistance of Subprocessors in providing access to relevant information needed to fulfill Customer's obligations under Applicable Data Protection Law.

4. Rights of Data Subjects. Processor will, to the extent legally permitted, promptly notify Customer if Processor receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of processing, right to be forgotten, data portability, objection to the processing, right to opt out of the sale of their personal information, or right not to be subject to an automated individual decision making. Taking into account the nature of the Processing, Processor shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to the Data Subject's request.

Docusign Envelope ID: D66DFAE3-4704-8067-813B-BB348A8864F7

5. **Limited use of Personal Data & personnel.** Except for the limited purposes required to provide the Services to Customer as set forth in the Services Agreement, (i) Processor will not acquire any rights in or to the Personal Data; and (ii) Processor and its Affiliates shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any contracted Subprocessor who may have access to the Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Personal Data, as strictly necessary for the purposes of the Services Agreement, and to comply with applicable data protection and privacy laws, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

6. **Subprocessors**.

a. **Appointment of Subprocessors**. Customer provides general consent to Processor to use of Subprocessors. Customer acknowledges and agrees that (a) Processor's Affiliates may be retained as Subprocessors; and (b) Processor and its Affiliates respectively may engage third-party Subprocessors in connection with the provision of the Services. Processor or its Affiliate(s) have entered into a written agreement with each Subprocessor containing data protection obligations not less protective than those in this DPA with respect to the protection of Personal Data to the extent applicable to the nature of the Services provided by such Subprocessor. Processor shall remain fully responsible to Customer for the performance of its Subprocessors in accordance with this DPA.

b. **List**. The current list of Subprocessors for the Services is available on the Grafana Labs website at: https://grafana.com/legal, which contains a mechanism for Customer to subscribe to notifications of any addition or replacement in Subprocessors. If Customer subscribes to such notifications, Processor will notify Customer of any such changes in Subprocessors through such mechanism. To subscribe, use the weblinks set forth in this Section 6.b.

c. **Objection**. Customer may object to Processor's use of a new Subprocessor by promptly notifying Processor in writing, not to exceed thirty (30) days of receipt of Processor's notice in accordance with the mechanism set out in Section 6(b), to privacy@grafana.com if based on reasonable grounds related to data protection. In such event, Processor will reasonably determine whether accommodations can be made available to Customer to avoid processing of Personal Data by the objected-to new Subprocessor without unduly burdening Customer. If Processor is unable to make available such accommodations within a reasonable period of time, which shall not exceed sixty (60) days from receipt of Customer's objection, then either party may terminate the applicable ordering document with respect only to the Services which cannot be provided by Processor without the use of the objected-to new Subprocessor by providing written notice to the other party. If no objection has been raised within thirty (30) days of receipt of Processor's notice in accordance with the mechanism set out in Section 6(b), Grafana Labs will deem Customer to have authorized the new Subprocessor.

7. **Special categories of Personal Data**. Customer (and its Affiliates) shall be solely responsible for compliance with data protection and privacy laws, as applicable to Customer (and its Affiliates), including any Personal Data that requires special handling or special categories of Personal Data such as, without limitation, that which relates to an individual's race or ethnicity, political opinions, religious or philosophical beliefs, trade-union membership, health, sex life, or personal finances. Customer shall use reasonable efforts to restrict transmission of any such special categories of Personal Data to the Grafana Product(s).

8. **Security of Personal Data.**

a. The Processor shall at a minimum implement the technical and organizational measures specified in Appendix 2 to ensure the security of the Personal Data. This includes protecting the Personal Data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to the Personal Data. In assessing the appropriate level of security, the parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the Data Subjects.

b. The Processor shall grant access to the Personal Data undergoing processing to members of its personnel only to the extent necessary for implementing, managing and monitoring of the Services Agreement. The Processor shall ensure that persons authorized to process the Personal Data received

have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

9. Personal Data Breach.

a. Grafana Labs will notify Customer without undue delay after detecting a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed by Grafana Labs (any such incident, a "Security Breach").

b. Such notification shall contain, at least
   (i) a description of the nature of the Security Breach (including, where possible, the categories and approximate number of Data Subjects and data records concerned);
   (ii) the details of a contact point where more information concerning the Personal Data breach can be obtained; and
   (iii) its likely consequences and the measures taken or proposed to be taken to address the Security Breach, including to mitigate its possible adverse effects.

c. Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

10. International Transfer of Data

a. **General**. Processor will abide by the requirements of Applicable Data Protection Law regarding the international transfer of Personal Data to Processor. Solely for the provision of Services to Customer under the Services Agreement, Personal Data may be transferred to and stored and/or Processed in any country in which Processor or its Subprocessors operate. All applicable transfers of Personal Data shall be governed by the applicable Cross Border Data Transfer Mechanisms which the parties hereby enter into and incorporate into this DPA as referenced in Schedule 2 (Cross Border Data Transfer Mechanisms).

b. **Data Transfer Assessment.** Processor's Services may require that some amount of Personal Data be transferred to the United States, and so Processor has compiled a Data Transfer Assessment, which can be found at https://grafana.com/legal.

11. Governmental queries. Grafana Labs will not disclose to any third party, any Personal Data, except, in each case, as necessary to maintain or provide the Services, or as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order). If a governmental body sends Grafana Labs a demand for Personal Data, Grafana Labs will attempt to redirect the governmental body to request that data directly from Customer. As part of this effort, Grafana Labs may provide Customer's basic contact information to the governmental body. If compelled to disclose Personal Data to a governmental body, then Grafana Labs will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Grafana Labs is legally prohibited from doing so.

12. Verification and audit. The parties acknowledge that Customer must be able to assess Grafana Labs' compliance with its obligations under Applicable Data Protection Law and this DPA, insofar as Grafana Labs is acting as a processor on behalf of Customer**.**

a. **Grafana Labs' Audit Program.** Grafana Labs uses external auditors to verify the adequacy of its security measures with respect to its processing of Personal Data. Such audits are performed at least once annually at Grafana Labs' expense by independent third-party security professionals at Grafana Labs' selection and result in the generation of a confidential audit report ("Audit Report"). A description of Grafana Labs' certifications and standards for audit of the Grafana Labs Services can be found at https://grafana.com/legal.

b. **Customer Audit.** Upon Customer's written request at reasonable intervals, and subject to reasonable confidentiality controls, Grafana Labs will make available to Customer a copy of Grafana Labs' most recent

Docusign Envelope ID: D66DFAE3-4704-8067-813B-BB348A8864F7

Audit Report. Customer agrees that any audit rights granted by Applicable Data Protection Law will be satisfied by these Audit Reports. To the extent that Grafana Labs' provision of an Audit Report does not provide sufficient information or Customer is required to respond to a regulatory authority audit, Customer agrees to a mutually agreed-upon audit plan with Grafana Labs that: (a) ensures the use of an independent third party; (b) provides notice to Grafana Labs in a timely fashion; (c) requests access only during business hours; (d) accepts billing to Customer at Grafana Labs' then-current rates; (e) occurs no more than once annually; (f) restricts its findings to only data relevant to Customer; and (g) obligates Customer, to the extent permitted by law or regulation, to keep confidential any information gathered that, by its nature, should be confidential

Docusign Envelope ID: D66DFAE3-4704-8067-813B-BB348A8864F7

APPENDIX 1 TO THE DPA – DETAILS OF PROCESSING

This Appendix 1 includes details of the Processing of Controller's Personal Data

- **Data Subjects:** The Personal Data to be sent through the Services is determined by the Controller, and may include, without limitation, data relating to its customers, employees, contractors, suppliers, and other personnel engaged to work for Controller or use the Services.
- **Categories of Personal Data:** The Personal Data to be sent through the Services is determined by the Controller, and may include name, business, contact information (including address, telephone numbers, mobile telephone numbers, web address data, email addresses), IP addresses, and online account details (including passwords and usernames).
- **Sensitive Information:** The Personal Data to be sent through the Services is determined by the Controller and is not expected to contain any Sensitive Information. Controller shall use reasonable efforts to restrict transmission of any Sensitive Information to Processor.
- **Processing Operations**: Processor processes Personal Data as necessary to provide the Services to Controller.
- **Period of Personal Data Retention:** Provider processes Personal Data for the duration described in the Services Agreement.
- **Subprocessors:** A current list of Subprocessors is set forth in Section 6 of this DPA.

Docusign Envelope ID: D66DFAE3-4704-8067-813B-BB348A8864F7

APPENDIX 2 TO THE DPA –
TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

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, Processor shall implement the measures outlined in the Services Agreement to ensure an appropriate level of security for the provision of the Services.

Where applicable, this Appendix 2 will serve as Annex II to the EU Standard Contractual Clauses and UK International Data Transfer Agreement.

SCHEDULE 2

CROSS BORDER DATA TRANSFER MECHANISMS

1. Definitions

- “EC” means the European Commission
- “EEA” means the European Economic Area
- "EU Standard Contractual Clauses” means the Standard Contractual Clauses approved by the European Commission in decision 2021/914.
- “UK International Data Transfer Agreement” means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022.

2. Cross Border Data Transfer Mechanisms.

2.1 Order of Precedence. In the event the Services are covered by more than one Transfer Mechanism, the transfer of Personal Data will be subject to a single Transfer Mechanism in accordance with the following order of precedence: (a) the EU Standard Contractual Clauses as set forth in Section 2.2 (EU Standard Contractual Clauses) of this Schedule 2; (b) the UK International Data Transfer Agreement as set forth in Section 2.3 (UK International Data Transfer Agreement) of this Schedule 2; and, if neither (a) nor (b) is applicable, then (c) other applicable data Transfer Mechanisms permitted under Applicable Data Protection Law.

2.2 EU Standard Contractual Clauses. The parties agree that the EU Standard Contractual Clauses will apply to Personal Data that is transferred via the Services from the EEA or Switzerland, either directly or via onward transfer, to any country or recipient outside the EEA or Switzerland that is: (a) not recognized by the European Commission (or, in the case of transfers from Switzerland, the competent authority for Switzerland) as providing an adequate level of protection for Personal Data. For data transfers from the EEA Area that are subject to the EU Standard Contractual Clauses, the EU Standard Contractual Clauses will be deemed entered into (and incorporated into this DPA by this reference) and completed as follows:

(a) Module Two (Controller to Processor) of the EU Standard Contractual Clauses will apply where Customer is a controller of Personal Data and Grafana Labs is processing Personal Data.

(b) Module Three (Processor to Processor) of the EU Standard Contractual Clauses will apply where Customer is a processor of Personal Data and Grafana Labs is processing Personal Data.

(c) For each Module, where applicable:

(i) in Clause 7 of the EU Standard Contractual Clauses, the optional docking clause will not apply;

(ii) in Clause 9 of the EU Standard Contractual Clauses, Option 2 will apply and the time period for prior notice of subprocessor changes will be as set forth in Section 6 (Subprocessors) of this DPA;

(iii) in Clause 11 of the EU Standard Contractual Clauses, the optional language will not apply;

(iv) in Clause 17 (Option 1), the EU Standard Contractual Clauses will be governed by Irish law;

Docusign Envelope ID: D66DFAE3-4704-8067-813B-BB348A8864F7

(v) in Clause 18(b) of the EU Standard Contractual Clauses, disputes will be resolved before the courts of Ireland;

(vi) in Annex I, Part A of the EU Standard Contractual Clauses:

- Data Exporter: Customer.
- Contact Details: The email address(es) designated by Customer in Customer's account via its notification preferences.
- Data Exporter Role: The Data Exporter's role is set forth in Section 2 (Processing of Personal Data) of this DPA.
- Signature and Date: By entering into the Services Agreement, Data Exporter is deemed to have signed these EU Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the Services Agreement.
- Data Importer: Grafana Labs Inc.
- Contact details: Grafana Labs Privacy Team – privacy@grafana.com.
- Data Importer Role: Data Processor.
- Signature and Date: By entering into the Services Agreement, Data Importer is deemed to have signed these EU Standard Contractual Clauses, incorporated herein, including their Annexes, as of the Effective Date of the Services Agreement.

(vii) in Annex I, Part B of the EU Standard Contractual Clauses:

- The categories of data subjects are described in Appendix 1 (Details of Processing) of this DPA.
- The Sensitive Information transferred is described in Appendix 1 (Details of Processing) of this DPA.
- The frequency of the transfer is a continuous basis for the duration of the Services Agreement.
- The nature of the processing is described in Appendix 1 (Details of Processing) of this DPA.
- The purpose of the processing is described in Appendix 1 (Details of Processing) of this DPA.
- The period for which the Personal Data will be retained is described in Appendix 1 (Details of Processing) of this DPA.

- For transfers to subprocessors, the subject matter, nature, and duration of the processing is set forth at https://grafana.com/legal.

(viii) in Annex I, Part C of the EU Standard Contractual Clauses: The Irish Data Protection Commission will be the competent supervisory authority.

(ix) Schedule 2 (Technical and Organizational Security Measures) of this DPA serves as Annex II of the EU Standard Contractual Clauses.

2.3 UK International Data Transfer Agreement. The parties agree that the UK International Data Transfer Agreement will apply to Personal Data that is transferred via the Services from the United Kingdom, either directly or via onward transfer, to any country or recipient outside of the United Kingdom that is not recognized by the competent United Kingdom regulatory authority or governmental body for the United Kingdom as providing an adequate level of protection for Personal Data. For data transfers from the United Kingdom that are subject to the UK International Data Transfer Agreement, the UK International Data Transfer Agreement will be deemed entered into (and incorporated into this Addendum by this reference) and completed as follows:

(a) In Table 1 of the UK International Data Transfer Agreement, the parties' details and key contact information are located in Section 2.2 (c)(vi) of this Schedule 2.

(b) In Table 2 of the UK International Data Transfer Agreement, information about the version of the Approved EU SCCs, modules and selected clauses which this UK International Data Transfer Agreement is appended to is located in Section 2.2 (EU Standard Contractual Clauses) of this Schedule 2.

(c) In Table 3 of the UK International Data Transfer Agreement:

1. The list of Parties is located in Section 2.2(c)(vi) of this Schedule 2.
2. The description of the transfer is set forth in Appendix 1 (Details of Processing) of this DPA.
3. Annex II is located in Appendix 2 (Technical and Organizational Security Measures) of this DPA.
4. The list of sub-processors is located at https://grafana.com/legal.

(d) In Table 4 of the UK International Data Transfer Agreement, both the Importer and the exporter may end the UK International Data Transfer Agreement in accordance with the terms of the UK International Data Transfer Agreement.

2.4 Conflict. To the extent there is any conflict or inconsistency between the EU Standard Contractual Clauses or UK International Data Transfer Agreement and any other terms in this Addendum, including Schedule 3 (Jurisdiction Specific Terms), or the Services Agreement, the provisions of the EU Standard Contractual Clauses or UK International Data Transfer Agreement, as applicable, will prevail.

Docusign Envelope ID: D66DFAE3-4704-8067-813B-BB348A8864F7

SCHEDULE 3

JURISDICTION SPECIFIC TERMS

1. Australia:

1.1 The definition of “Applicable Data Protection Law” includes the Australian Privacy Principles and the Australian Privacy Act (1988).

1.2 The definition of “Personal Data” includes “Personal Information” as defined under Applicable Data Protection Law.

1.3 The definition of “Sensitive Information” includes “Sensitive Information” as defined under Applicable Data Protection Law.

2. Brazil:

2.1 The definition of “Applicable Data Protection Law” includes the Lei Geral de Proteção de Dados (LGPD).

2.2 The definition of “Security Breach” includes a security incident that may result in any relevant risk or damage to data subjects.

2.3 The definition of “processor” includes “operator” as defined under Applicable Data Protection Law.

3. California:

3.1 The definition of “Applicable Data Protection Law” includes the California Consumer Privacy Act (CCPA) and, beginning January 1, 2023, the California Privacy Rights Act (CPRA).

3.2 The definition of “Personal Data” includes “Personal Information” as defined under Applicable Data Protection Law.

3.3 The definition of “Data Subject” includes “Consumer” as defined under Applicable Data Protection Law. Any data subject rights, as described in Section 4 (Rights of Data Subjects) of this DPA, include any Consumer rights. In regards to data subject requests, Grafana Labs can only verify a request from Customer and not from Customer’s end user or any third party.

3.4 The definition of “controller” includes “Business” as defined under Applicable Data Protection Law.

3.5 The definition of “processor” includes “Service Provider” as defined under Applicable Data Protection Law.

3.6 Grafana Labs will process, retain, use, and disclose Personal Data only as necessary to provide the Services under the Services Agreement, which constitutes a business purpose. Grafana Labs agrees not to (a) sell (as defined by the CCPA) Customer’s Personal Data or Customer end users’ Personal Data; (b) retain, use, or disclose Customer’s Personal Data for any commercial purpose (as defined by the CCPA) or other purpose other than for the specific purpose of providing the Services; or (c) retain, use, or disclose Customer’s Personal Data outside of the direct business relationship between the parties as set forth in the Services Agreement. Additionally, beginning January 1, 2023, Grafana Labs: (a) shall not share (as defined in the CPRA) Customer’s Personal Data; (b) shall not

combine Customer's Personal Data with other Personal Information (as defined in the CPRA) received from any other source, except as otherwise permitted by the CPRA or its regulations; (c) shall provide the same level of privacy protection as is required by the CPRA; (d) shall notify Customer promptly in writing if Grafana Labs makes a determination that it can no longer meet its obligations under the CPRA; (e) grants Customer the right, upon notice, to take reasonable and appropriate steps to stop and remediate Grafana Labs' unauthorized use of Customer's Personal Data and to take reasonable and appropriate steps to ensure that Grafana Labs uses the Customer's Personal Data in a manner consistent with Customer's CPRA obligations. Grafana Labs certifies that it understands its obligations under Applicable Data Protection Law and this Section 3.6 and will comply with them.

3.7 Grafana Labs certifies that its subprocessors, as described in Section 6 (Subprocessors) of this DPA, are Service Providers under Applicable Data Protection Law, with whom Grafana Labs has entered into a written contract that includes terms substantially similar to this DPA. Grafana Labs conducts appropriate due diligence on its subprocessors.

3.8 Grafana Labs will implement and maintain reasonable security procedures and practices appropriate to the nature of the Personal Data it processes designed to protect the Personal Data from unauthorized or illegal access, destruction, use, modification, or disclosure as set forth in Section 8 (Security of Personal Data) of this DPA.

4. Canada:

4.1 The definition of "Applicable Data Protection Law" includes the Federal Personal Information Protection and Electronic Documents Act (PIPEDA).

4.2 Grafana Labs' subprocessors, as described in Section 6 (Subprocessors) of this DPA, are third parties under Applicable Data Protection Law, with whom Grafana Labs has entered into a written contract that includes terms substantially similar to this DPA. Grafana Labs has conducted appropriate due diligence on its subprocessors.

4.3 Grafana Labs will implement technical and organizational measures as set forth in Section 8 (Security of Personal Data) of this DPA.

5. European Economic Area (EEA):

5.1 The definition of "Applicable Data Protection Law" includes the General Data Protection Regulation (EU 2016/679) ("*GDPR*").

5.2 When Grafana Labs engages a subprocessor under Section 6 (Subprocessors) of this DPA, it will:

(a) require any appointed subprocessor to protect the Personal Data to the standard required by Applicable Data Protection Law, such as including the same data protection obligations referred to in Article 28(3) of the GDPR, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR, and

(b) require any appointed subprocessor to (i) agree in writing to only process Personal Data in a country that the European Union has declared to have an "adequate" level of protection or (ii) only process Personal Data on terms equivalent to the EU Standard Contractual Clauses or pursuant to a Binding Corporate Rules approval granted by competent European Union data protection authorities.

5.3 Notwithstanding anything to the contrary in this DPA or in the Services Agreement (including, without limitation, either party's indemnification obligations), neither party will be responsible for any

GDPR fines issued or levied under Article 83 of the GDPR against the other party by a regulatory authority or governmental body in connection with such other party's violation of the GDPR.

6. Israel:

6.1 The definition of "Applicable Data Protection Law" includes the Protection of Privacy Law (PPL).

6.2 The definition of "controller" includes "Database Owner" as defined under Applicable Data Protection Law.

6.3 The definition of "processor" includes "Holder" as defined under Applicable Data Protection Law.

6.4 Grafana Labs will require that any personnel authorized to process Personal Data comply with the principle of data secrecy and have been duly instructed about Applicable Data Protection Law. Such personnel sign confidentiality agreements with Grafana Labs in accordance with Section 5 (Limited use of Personal Data & personnel) of this DPA.

6.5 Grafana Labs must take sufficient steps to ensure the privacy of data subjects by implementing and maintaining the security measures as specified in Section 8 (Security of Personal Data) of this DPA and complying with the terms of the Services Agreement.

6.6 Grafana Labs must ensure that the Personal Data will not be transferred to a subprocessor unless such subprocessor has executed an agreement with Grafana Labs pursuant to Section 6 (Processors) of this DPA.

7. Japan:

7.1 The definition of "Applicable Data Protection Law" includes the Act on the Protection of Personal Information (APPI).

7.2 The definition of "Personal Data" includes "Personal Information" as defined under Applicable Data Protection Law.

7.3 The definition of "controller" includes "Business Operator" as defined under Applicable Data Protection Law. As a Business Operator, Grafana Labs is responsible for the handling of Personal Data in its possession.

7.4 The definition of "processor" includes a business operator entrusted by the Business Operator with the handling of Personal Data in whole or in part (also a "trustee"), as described under Applicable Data Protection Law. As a trustee, Grafana Labs will ensure that the use of the entrusted Personal Data is securely controlled.

8. Mexico:

8.1 The definition of "Applicable Data Protection Law" includes the Federal Law for the Protection of Personal Data Held by Private Parties and its Regulations (FLPPIPPE).

8.2 When acting as a processor, Grafana Labs will:

(a) treat Personal Data in accordance with Customer's instructions set forth in Section 2 (Processing

Docusign Envelope ID: D66DFAE3-4704-8067-813B-BB348A8864F7

of Personal Data) of this DPA;

(b) process Personal Data only to the extent necessary to provide the Services;

(c) implement security measures in accordance with Applicable Data Protection Law and Section 8 (Security of Personal Data) of this DPA;

(d) keep confidentiality regarding the Personal Data processed in accordance with the Services Agreement;

(e) delete all Personal Data in accordance with the Services Agreement; and

(f) only transfer Personal Data to subprocessors in accordance with Section 6 (Subprocessors) of this DPA.

9. Singapore:

9.1 The definition of “Applicable Data Protection Law” includes the Personal Data Protection Act 2012 (PDPA).

9.2 Grafana Labs will process Personal Data to a standard of protection in accordance with the PDPA by implementing adequate technical and organizational measures as set forth in Section 8 (Security of Personal Data) of this DPA and complying with the terms of the Services Agreement.

10. Switzerland:

10.1 The definition of “Applicable Data Protection Law” includes the Swiss Federal Act on Data Protection.

10.2 When Grafana Labs engages a subprocessor under Section 6 (Subprocessors) of this DPA, it will:

(a) require any appointed subprocessor to protect the Personal Data to the standard required by Applicable Data Protection Law, such as including the same data protection obligations referred to in Article 28(3) of the GDPR, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR, and

(b) require any appointed subprocessor to (i) agree in writing to only process Personal Data in a country that the European Union has declared to have an “adequate” level of protection or (ii) only process Personal Data on terms equivalent to the EU Standard Contractual Clauses or pursuant to a Binding Corporate Rules approval granted by competent European Union data protection authorities.

11. United Kingdom (UK):

11.1 References in this DPA to GDPR will to that extent be deemed to be references to the corresponding laws of the United Kingdom (including the UK GDPR and Data Protection Act 2018).

11.2 When Grafana Labs engages a subprocessor under Section 6 (Subprocessors) of this DPA, it will:

(a) require any appointed subprocessor to protect the Personal Data to the standard required by Applicable Data Protection Law, such as including the same data protection obligations referred to in Article 28(3) of the GDPR, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR; and

(b) require any appointed subprocessor to (i) agree in writing to only process Personal Data in a country that the United Kingdom has declared to have an “adequate” level of protection or (ii) only process Personal Data on terms equivalent to the UK International Data Transfer Agreement or pursuant to a Binding Corporate Rules approval granted by competent United Kingdom data protection authorities.

11.3 Notwithstanding anything to the contrary in this DPA or in the Services Agreement (including, without limitation, either party’s indemnification obligations), neither party will be responsible for any UK GDPR fines issued or levied under Article 83 of the UK GDPR against the other party by a regulatory authority or governmental body in connection with such other party’s violation of the UK GDPR.