Updated: December 2025

Data Processing Addendum

This Data Processing Addendum ("**DPA**") governs Magniv Inc. DBA PromptLayer's ("**PromptLayer**") processing of Customer Data provided by Customer to PromptLayer through PromptLayer's Services under the terms of the PromptLayer Terms of Use (located at https://promptlayer.com/termsofservice), and the Sales Agreement or other agreement between Customer and PromptLayer governing Customer's use of the Services (the "**Agreement**"), and is hereby incorporated into the Agreement. If and to the extent language in this DPA conflicts with the Agreement, the conflicting terms in this DPA shall control. Capitalized terms not defined in this DPA have the meaning set forth in the Agreement. For the purposes of this DPA only, "**Customer**" includes any entity that (a) has entered into a Sales Agreement with PromptLayer (b) its employees and contractors authorized to use the Services provided by Promptlayer (and subject to any terms and conditions on such use), and (c) any affiliate entities of the entity entering into a Sales Agreement who Promptlayer provides express written consent to use the Promptlayer Services.

PromptLayer and Customer each agree to comply with their respective obligations under applicable data privacy and data protection laws (collectively, "**Data Protection Laws**") in connection with the Services. Data Protection Laws may include, but are not limited to, depending on the circumstances, Cal. Civ. Code §§ 1798.100 et seq., as amended by the California Privacy Rights Act of 2020 (the California Consumer Privacy Act) ("**CCPA**"), Colo. Rev. Stat. §§ 6-1-1301 et seq. (the Colorado Privacy Act) ("**CPA**"), Connecticut's Data Privacy Act ("**CTDPA**"), Utah Code Ann. §§ 13-61-101 et seq. (the Utah Consumer Privacy Act) ("**UCPA**"), VA Code Ann. §§ 59.1-575 et seq. (the Virginia Consumer Data Protection Act) ("**VCDPA**") (collectively "**U.S. Privacy Laws**"), and the United Kingdom and/or European Union General Data Protection Regulation (Regulation (EU) 2016/679) (collectively the "**GDPR**"), and applicable subordinate legislation and regulations implementing those laws.

In connection with the Agreement, Customer is the person that determines the purposes and means for which Customer Data (as defined below) is processed (a "**Data Controller**"), whereas PromptLayer processes Customer Data in accordance with the Data Controller's instructions and on behalf of the Data Controller (as a "**Data Processor**"). "**Data Controller**" and "**Data Processor**" also mean the equivalent concepts under Data Protection Laws. For the purposes of the Agreement and this DPA, (i) "**Personal Data**" has the meaning assigned to the term "personal data" or "personal information" under applicable Data Protection Laws; and (ii) "**Customer Data**" means Personal Data that Customer provides to PromptLayer that PromptLayer processes on

behalf of Customer to provide the Services. PromptLayer will process Customer Data as Customer's Data Processor to provide or maintain the Services and for the purposes set forth in this DPA, the Agreement and/or in any other applicable agreements between Customer and PromptLayer.

1. Processing Requirements

As a Data Processor, PromptLayer agrees to:

a. process Customer Data only (i) on Customer's behalf for the purpose of providing and supporting PromptLayer's Services (including to provide insights, reporting, analytics, and platform abuse, trust and safety monitoring) and (ii) in compliance with the written instructions received from Customer or pursuant to Customer's use of the Services.

b. promptly inform Customer in writing if PromptLayer cannot comply with the requirements of this DPA;

c. not provide Customer with remuneration in exchange for Customer Data from Customer. The parties acknowledge and agree that Customer has not "sold" (as such term is defined by the CCPA) Customer Data to PromptLayer;

d. not "sell" (as such term is defined by U.S. Privacy Laws) or "share" (as such term is defined by the CCPA) Personal Data;

e. inform Customer promptly if, in PromptLayer's opinion, Promptlayer becomes aware it has received an instruction from Customer that violates applicable Data Protection Laws;

f. require (i) persons employed by it and (ii) other persons engaged to perform on PromptLayer's behalf to be subject to a duty of confidentiality with respect to the Customer Data and to comply with the data protection obligations applicable to PromptLayer under the Agreement and this DPA;

g. engage the organizations or persons listed in the SOC2 audit report, provided on request to Customer, as may be updated from time to time, to process Customer Data (each a "**Subprocessor,**" and the list currently included but not limited to, Calendly, Datadog, Github, Google Cloud Platform, Google Drive, Google Workspace, Notion, Sentry, Slack, Vanta, together, the "**Subprocessor List**") to help PromptLayer satisfy its obligations in accordance with this DPA or to delegate all or part of the processing activities to such Subprocessors. Customer hereby consents to the use of such Subprocessors. If Customer subscribes to email notifications as provided on the Subprocessor List website, then PromptLayer will notify Customer of any changes

PromptLayer intends to make to the Subprocessor List at least 15 days before the changes take effect (which may be via email, a posting, or notification on an online portal for our services or other reasonable means). In the event that Customer does not wish to consent to the use of such additional Subprocessor, Customer must notify PromptLayer that Customer does not consent within fifteen (15) days of the notification of the addition of any Subprocessor and such notice must include the reasonable grounds relating to the protection of Customer Data by following the instructions set forth in the Subprocessor List or by contacting privacy@promptlayer.com. Upon receipt of such notice, PromptLayer shall have the right to cure the objection through one of the following options: (i) PromptLayer will cancel its plans to use the Subprocessor with regards to processing Customer Data or will offer an alternative to provide its Services or services without such Subprocessor, which may occur for just the Customer or all PromptLayer customers; (ii) PromptLayer may take the corrective steps requested by Customer in Customer objection notice and proceed to use the Subprocessor; (iii) PromptLayer may cease to provide, or Customer may agree not to use whether temporarily or permanently, the particular aspect or feature of the PromptLayer Services or services that would involve the use of such Subprocessor; or (iv) Customer may cease providing Customer Data to PromptLayer for processing involving such Subprocessor. If none of the above options are commercially feasible, in PromptLayer's reasonable judgment, and the objection(s) have not been resolved to the reasonable satisfaction of the parties within thirty (30) days of PromptLayer's receipt of Customer's objection notice, then either party may terminate any Agreements, subscriptions, order forms or usage regarding the Services that cannot be provided without the use of the new Subprocessor for cause. In such case, Customer will be refunded any pre-paid fees for the applicable subscriptions, order forms, or usage to the extent they cover periods or terms following the date of such termination. Such termination right is Customer's sole and exclusive remedy if Customer objects to any new Subprocessor. Should Customer fail to elect to provide any reasonable written objection to the use of any Subprocessor within fifteen days of written notice that such Subprocessor is being engaged, Customer shall be deemed to have accepted the use of such Subprocessor. PromptLayer shall enter into contractual arrangements with each Subprocessor binding them to provide a reasonably comparable level of data protection and information security to that required for herein.;

h. upon reasonable request no more than once per year, provide Customer with PromptLayer's privacy and security policies and other such information necessary to demonstrate compliance with the obligations set forth in this DPA and applicable Data Protection Laws;

i. where required by law and upon reasonable notice, request, and appropriate confidentiality agreements, cooperate with assessments, audits, or other steps performed by or on behalf of Customer at Customer's sole expense and in a manner that is minimally disruptive to PromptLayer's business that are necessary to confirm that PromptLayer is processing Customer Data in a manner consistent with this DPA. For the avoidance of doubt, any expenses incurred as part of any such assessment or audit by PromptLayer shall be charged to Customer and Customer agrees to promptly reimburse Promptlayer for any such expenses not more than fifteen (15) days after being invoiced by Promptlayer. Where permitted by law, in lieu of such assessment or audit, PromptLayer shall, in its sole discretion, instead have the option to make available to Customer a summary of the results of a third-party audit or certification reports relevant to PromptLayer's compliance with this DPA, such as a SOC 2 Type 2 report. Such results, and/or the results of any such assessments, audits, or other steps shall be the Confidential Information of PromptLayer;

j. to the extent that Customer permits or instructs PromptLayer to process Customer Data subject to U.S. Privacy Laws in a de-identified, anonymized, and/or aggregated form as part of the Services, PromptLayer shall (i) attempt to adopt reasonable measures to prevent such deidentified data from being used to infer information about, or otherwise being linked to, a particular natural person or household; (ii) not attempt to re-identify the information, except that PromptLayer may attempt to reidentify the information solely for the purpose of determining whether its de-identification processes comply with Data Protection Laws or are functioning as intended; and (iii) before sharing de-identified data with any other party, including Subprocessors, contractually obligate any such recipients to comply with the requirements of this provision;

k. where the Customer Data is subject to the CCPA, not (i) retain, use, disclose, or otherwise process Customer Data except as necessary for the business purposes specified in the Agreement or this DPA; (ii) retain, use, disclose, or otherwise process Customer Data in any manner outside of the direct business relationship between PromptLayer and Customer; or (iii) combine any Customer Data with Personal Data that PromptLayer receives from or on behalf of any other third party or collects from PromptLayer's own interactions with individuals, provided that PromptLayer may so combine Customer Data for a purpose permitted under the CCPA if directed to do so by Customer or as otherwise permitted by the CCPA;

l. where required by law, grant Customer the rights to (i) take reasonable and appropriate steps to ensure that PromptLayer uses Customer Data in a manner consistent with Data Protection Laws by exercising the audit provisions set forth in this DPA above; and (ii) stop and remediate unauthorized use of Customer Data, for

example by requesting that PromptLayer provide written confirmation that applicable Customer Data has been deleted.

m. Customer acknowledges that in certain situations Third Party Artificial Intelligence Applications used by Customer may act as Subprocessors of PromptLayer.

l. Customer also agrees and acknowledges Customer, not PromptLayer shall have primary responsibility for ensuring all Customer Data and the Services are used in a way that complies with any Data Protection Laws or other applicable laws and shall immediately cease providing PromptLayer and the Services if the use of such Services or the providing of such Customer Data would violate any laws. To the extent PromptLayer, its employees, contractors, directors, Subprocessors, directors, shareholders, or other affiliates suffer any damages arising out of or otherwise related to Customer providing Customer Data to PromptLayer or otherwise using the Services.

2. Notice to Customer

PromptLayer will inform Customer if PromptLayer becomes aware of:

a. any legally binding request for disclosure of Customer Data by a law enforcement authority, unless PromptLayer is otherwise forbidden by law to inform Customer, for example, to preserve the confidentiality of an investigation by law enforcement authorities;

b. any notice, inquiry, or investigation by an independent public authority established by a member state pursuant to Article 51 of the GDPR (a “Supervisory Authority”) with respect to Customer Data; or

c. any complaint or request (in particular, requests for access to, rectification or blocking of Customer Data) received directly from Customer’s data subjects or customers. PromptLayer will not respond to any such request without Customer’s prior written authorization unless it otherwise believes it is obligated to do so or doing so is in its best interests, in which case it will provide Customer with notice of such response.

3. Assistance to Customer

PromptLayer will provide reasonable assistance to Customer regarding:

a. information necessary, taking into account the nature of the processing, to respond to requests received pursuant to Data Protection Laws from Customer’s data subjects in respect of access to or the rectification, erasure, restriction, portability, objection, blocking, or deletion of Customer Data that PromptLayer processes for Customer. In the event that a data subject sends such a request directly to PromptLayer, PromptLayer will promptly send such request to Customer;

b. the investigation of any breach of PromptLayer's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to Customer Data processed by PromptLayer for Customer (a "Personal Data Breach"); and

c. where appropriate, the preparation of data protection impact assessments with respect to the processing of Customer Data by PromptLayer and, where necessary, carrying out consultations with any supervisory authority with jurisdiction over such processing.

4. Required Processing

If PromptLayer becomes aware that it is required by Data Protection Laws to process any Customer Data for a reason other than in connection with the Agreement, PromptLayer will inform Customer of this requirement in advance of any such processing, unless legally prohibited.

5. Security

PromptLayer will:

a. attempt to maintain commercially reasonable and appropriate organizational and technical security measures, including but not limited to those measures described in Exhibit B to this DPA (including with respect to personnel, facilities, hardware and software, storage and networks, access controls, monitoring and logging, vulnerability and breach detection, incident response, and encryption) to protect against unauthorized or accidental access, loss, alteration, disclosure or destruction of Customer Data and to protect the rights of the subjects of that Customer Data;

b. attempt to take commercially reasonable steps to confirm that PromptLayer personnel are protecting the security, privacy and confidentiality of Customer Data consistent with the requirements of this DPA; and

c. notify Customer of any Personal Data Breach by PromptLayer, its Subprocessors, or any other third parties acting on PromptLayer's behalf without undue delay after PromptLayer becomes aware of such Personal Data Breach.

6. Obligations of Customer

a. Customer represents, warrants and covenants that it has and shall maintain throughout the term all necessary rights, consents and authorizations to provide the Customer Data to PromptLayer and to authorize PromptLayer to use, disclose, retain and otherwise process Customer Data as contemplated by this DPA, the Agreement and/or other processing instructions provided to PromptLayer.

b. Customer shall comply with all applicable Data Protection Laws and ensure all use of the Services and sharing of Customer Data with PromptLayer also complies with all applicable Data Protection Laws and any other rules, regulations, and laws.

c. Customer shall reasonably cooperate with PromptLayer to assist PromptLayer in performing any of its obligations with regard to any requests from Customer's data subjects.

d. Notwithstanding the obligations contained in Section 5 of this DPA, Customer acknowledges and agrees that it, rather than PromptLayer, is solely responsible for ensuring all configurations, implementation of any configuration, API, and integration, design decisions, and use of the Services occurs in a secure manner that complies with applicable Data Protection Laws.

e. Customer shall not provide Customer Data to PromptLayer except through agreed mechanisms and in a manner compliant with all Data Protection Laws. For example, Customer shall not include Customer Data other than technical contact information, or in technical support tickets, transmit user Customer Data to PromptLayer by email. Without limitation to the foregoing, Customer represents, warrants and covenants that it shall only transfer Customer Data to PromptLayer using secure, reasonable, and legally-appropriate mechanisms.

f. Customer shall not take any action that would (i) render the provision of Customer Data to PromptLayer a "sale" under U.S. Privacy Laws or a "share" under the CCPA (or equivalent concepts under U.S. Privacy Laws); or (ii) render PromptLayer not a "service provider" under the CCPA or "processor" under U.S. Privacy Laws.

7. International Data Transfers

a. PromptLayer will process Customer Data provided by Customer that originates in the EEA or Switzerland. To the extent that PromptLayer transfers Customer Data to jurisdictions that do not provide the same level of data protection, it will do so on the basis of intra-group agreements that incorporate appropriate transfer mechanism provisions to protect Customer Data. Such mechanisms may include the Standard Contractual Clauses adopted by the EU Commission on June 4, 2021 (as may be amended, updated or replaced from time to time) ("**EU SCCs**") or an adequacy decision issued by the European Commission under Article 45 GDPR.

b. PromptLayer will process Customer Data provided by Customer located in the UK in accordance with the EU SCCs as amended by the UK addendum to the EU SCCs issued by the Information Commissioner under section 119A(1) of the Data Protection Act 2018 ("**UK Addendum**") which are deemed entered into (and incorporated into this

DPA by this reference) and completed as follows (each as amended by the UK Addendum, where relevant and applicable): i. Module Two (Controller to Processor) of the EU SCCs apply when Customer is a controller and PromptLayer is processing Customer Data as a processor. ii. Module Three (Processor to Sub-Processor) of the EU SCCs apply when Customer is a processor and PromptLayer is processing Customer Data as a sub-processor.

c. For each module of the EU SCCs, where applicable, the following applies: i. The optional docking clause in Clause 7 does not apply; ii. In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of sub-processor changes shall be as set forth in Section 1(g) of this DPA. iii. In Clause 11, the optional language does not apply; iv. All square brackets in Clause 13 are hereby removed; v. In Clause 17 (Option 1), the EU SCCs will be governed by the laws of England and Wales; vi. In Clause 18(b), disputes will be resolved before the courts of England and Wales; vii. Exhibit A to this DPA contains the information required in Annex I and Annex III of the EU SCCs; viii. Exhibit B to this DPA contains the information required in Annex II of the EU SCCs; and

d. The parties will comply with the terms of Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B1.0 . The parties also agree (i) that the information included in Part 1 of the UK Addendum is as set out in Exhibit A to this DPA and (ii) that either party may end the UK Addendum as set out in Section 19 of the UK Addendum.

8. Term; Data Return and Deletion

This DPA shall remain in effect as long as PromptLayer carries out Customer Data processing operations on Customer's behalf or until the termination of the Agreement, whichever is sooner. PromptLayer will retain Customer Data sent through the API for a maximum of thirty (30) days, after which it will be deleted, except where PromptLayer is required to retain copies under applicable laws, in which case PromptLayer will isolate and protect that Customer Data from any further processing except to the extent required by applicable laws or except as otherwise authorized or described in the Agreement or any other agreement between PromptLayer and Customer. PromptLayer will retain Customer Data during the term of the Agreement, unless otherwise stated in the Agreement or Order Form. On the termination of the DPA, PromptLayer will direct each Subprocessor to delete the Customer Data within thirty (30) days of the DPA's termination, unless prohibited by law or commercially unreasonable or unfeasible, or otherwise set forth in the Agreement. For clarity, PromptLayer may continue to process information derived from Customer Data that has been deidentified, anonymized, and/or aggregated such that the data is no longer considered Personal Data under applicable

Data Protection Laws and in a manner that does not identify individuals or Customer to improve PromptLayer's systems and services to the maximum extent allowed by law.

Exhibit A

A. LIST OF PARTIES

Data exporter(s): the Customer using the Services as identified in the Agreement and any associated documents.

Data importer(s):

Name: Magniv, Inc.

Address: 43 W 29th St Floor 3, New York, NY 10001

Contact Person's name, position, and contact details: Jonathan Pedoeem, jon@promptlayer.com

Activities relevant to the data transferred under these Clauses: The performance of the Services described in the agreement to which this is attached and any other agreements entered into by and between Customer and PromptLayer.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Any entity or individual provided by Customer to Promptlayer through the use of the Services.

Categories of personal data transferred

Name, contact information, demographic information, or other information provided by the user in unstructured data.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

No sensitive data is intended to be transferred unless the Customer includes it in unstructured data (in violation of this DPA).

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous.

Nature of the processing

The performance of the Services described in the Agreement to which this Exhibit is attached.

Purpose(s) of the data transfer and further processing

The performance of the Services described in the Agreement to which this exhibit is attached.

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

During the term of the Agreement or as otherwise set forth in this DPA or Agreement.

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

The performance of the Services described in the Agreement to which this Exhibit is attached and of the nature and duration as set forth in the DPA and Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Information Commissioner's Office ("ICO").

Exhibit B

TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

INTRODUCTION

PromptLayer takes security seriously and maintains an information security program designed to attempt to safeguard its systems, data, and Customer Data. This Exhibit describes the information security program and security standards that PromptLayer maintains with respect to the Services and handling of data submitted by or on behalf of Customer of the Services (the "Customer Data"). Capitalized terms not defined in this Exhibit have the meanings given in the DPA or Agreement.

SECURITY MEASURES

Corporate Identity, Authentication, and Authorization Controls. PromptLayer maintains industry-standard practices for authenticating and authorizing internal employee and service access, including the following measures:

- PromptLayer uses single sign-on (SSO) to authenticate to third-party services used in the delivery of the Services. Role-Based Access Controls (RBAC) are used when provisioning internal access to the Services;
- Mandatory multi-factor authentication is used for authenticating to PromptLayer's identity provider.
- Unique login identifiers are assigned to each user;
- Established review and approval processes for any access requests to services storing Customer Data;
- Periodic access audits designed to ensure access levels are appropriate for the roles each user performs;
- Established procedures for promptly revoking access rights upon employee separation;
- Established procedures for reporting and revoking compromised credentials such as passwords and API keys); and
- Established password reset procedures, including procedures designed to verify the identity of a user prior to a new, replacement, or temporary password.

Customer Identity, Authentication, and Authorization Controls. PromptLayer maintains industry standard practices for authenticating and authorizing customers to the Services, including the following measures:

- Use of a third-party identity access management service to manage Customer identity, meaning PromptLayer does not store user-provided passwords on users' behalf; and
- Logically separating Customer Data by organization account using unique identifiers. Within an organization account, unique user accounts are supported.
- Cloud Infrastructure and Network Security. PromptLayer maintains industry best practices for securing and operating its cloud infrastructure, including the following measures:
- Separate production and non-production environments;
- Primary backend resources are deployed behind a VPN.

- The Services are routinely audited for security vulnerabilities.
- Application secrets and service accounts are managed by a secrets management service;
- Network security policies and firewalls are configured for least-privilege access against a pre-established set of permissible traffic flows. Non-permitted traffic flows are blocked; and
- Services logs are monitored for security and availability.

System and Workstation Control. PromptLayer maintains industry standard practices for securing PromptLayer's corporate systems, including laptops and on-premises infrastructure, including:

- Endpoint management of corporate workstations;
- Endpoint management of mobile devices;
- Automatic application of security configurations to workstations;
- Mandatory patch management; and
- Maintaining appropriate security logs.

Data Access Control. PromptLayer maintains industry standard practices for preventing authorized users from accessing data beyond their authorized access rights and for preventing the unauthorized input, reading, copying, removal, modification, or disclosure of data. Such measures include the following:

- Employee access to the Services follows the principle of least privilege. Only employees whose job function involves supporting the delivery of Services are credentialed to the Services environment; and
- Customer Data submitted to the Services is only used in accordance with the terms of the DPA, Agreement, and any other applicable contractual agreements in place with Customer.

Disclosure Control. PromptLayer maintains industry standard practices for preventing the unauthorized access, alteration, or removal of data during transfer, and for securing and logging all transfers. Such measures include:

- Encryption of data at rest in production datastores using strong encryption algorithms;
- Encryption of data in transit;

- Audit trail for all data access requests for production datastores;
- Full-disk encryption required on all corporate workstations;
- Device management controls required on all corporate workstations;
- Restrictions on use of portable or removable media; and
- Customer Data can be deleted upon request.

Availability control. PromptLayer maintains industry standard practices for maintaining Services functionality through accidental or malicious intent, including:

- Ensuring that systems may be restored in the event of an interruption;
- Ensuring that systems are functioning and faults are reported; and
- Anti-malware and intrusion detection/prevention solutions implemented comprehensively across our environment.

Segregation control. PromptLayer maintains industry standard practices for separate processing of data collected for different purposes, including:

- Logical segregation of Customer Data;
- Restriction of access to data stored for different purposes according to staff roles and responsibilities;
- Segregation of business information system functions; and
- Segregation of testing and production information system environments.

Risk Management. PromptLayer maintains industry standard practices for detecting and managing cybersecurity risks, including:

- Threat modeling to document and triage sources of security risk for prioritization and remediation;
- Penetration testing is conducted on the Services at least annually, and any remediation items identified are resolved as soon as possible on a timetable commensurate with the associated risk. Upon request, PromptLayer will provide summary details of the tests performed and whether the identified issues have been resolved;
- Annual engagements of a qualified, independent external auditor to conduct periodic reviews of PromptLayer's security practices against recognized audit

standards, including SOC 2 Type II certification audits. Upon reasonable request, PromptLayer will provide summary details; and

- A vulnerability management program designed to ensure the prompt remediation of vulnerabilities affecting the Services.

Personnel. PromptLayer maintains industry standard practices for vetting, training, and managing personnel with respect to security matters, including:

- Background checks, where legally permissible, of employees with access to Customer Data or supporting other aspects of the Services;
- Annual security training for employees, and supplemental security training as appropriate.

Physical Access Control. PromptLayer maintains industry standard practices for preventing unauthorized physical access to PromptLayer facilities.

Third Party Risk Management. PromptLayer maintains industry standard practices for managing third-party security risks, including with respect to any subprocessor or subcontractor to whom PromptLayer provides Customer Data, including the following measures:

- Written contracts designed to ensure that any agent agrees to maintain reasonable and appropriate safeguards to protect Customer Data; and
- Vendor Security Assessments: All third parties undergo a formal vendor assessment process maintained by PromptLayer's Security team.

Security Incident Response. PromptLayer maintains a security incident response plan for responding to and resolving events that compromise the confidentiality, availability, or integrity of the Services or Customer Data, including the following:

- PromptLayer aggregates system logs for security and general observability from a range of systems to facilitate detection and response; and
- If PromptLayer becomes aware that a Personal Data Breach has occurred, PromptLayer will notify Customer in accordance with the DPA.

Security Evaluations. PromptLayer performs regular security and vulnerability testing to assess whether key controls are implemented properly and are effective as measured against industry security standards and its policies and procedures, and to ensure continued compliance with obligations imposed by law, regulation, or contract with respect to the security of Customer Data as well as the maintenance and structure of PromptLayer's information systems.