Data Processing Addendum

This Data Processing Addendum (“**DPA**”) forms part of the Master Services Agreement (or other similarly titled written or electronic agreement addressing the same subject matter) (“**Agreement**”), between

1. Customer (as defined in the Agreement) and
2. **CodeRabbit Inc.** (“**CodeRabbit**”),

under which CodeRabbit provides Customer with the software and services described therein (the “**Services**”). CodeRabbit and Customer are individually referred to as a “**Party**” and collectively as the “**Parties**”. This DPA is hereby incorporated by reference into and made a part of the Agreement.

1. **Definitions.** Terms not otherwise defined herein shall have the meaning given to them in the Agreement.

    1. “**Applicable Data Protection Laws**” means all data protection and privacy laws and regulations applicable to CodeRabbit’s provision of the Services to Customer, including, without limitation and if and to the extent applicable, European Data Protection Laws and US Data Protection Law, as the same may be amended, superseded or replaced.

    2. “**CodeRabbit Account Data**” means Customer Data that is also Personal Data and relates to CodeRabbit’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. CodeRabbit Account Data also includes any Customer Data CodeRabbit may need to collect for the purpose of managing its relationship with Customer (including communications and support), identity verification, or as otherwise required by applicable laws and regulations.

    3. "**CodeRabbit Usage Data**" means Services usage data collected and Processed by CodeRabbit 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 security threats and malicious activity, as may be more specifically set forth in the Agreement.

    4. “**Controller**” means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processprocessing of personal data.

    5. “**Customer Data**” means any Personal Data Processed by CodeRabbit in accordance with Section 2 of this DPA in connection with the Services, and as more particularly described in Annex 1 [2] of this DPA (as applicable).

    6. “**Data Transfer**” means a transfer of Customer Data from the Controller to the Processor, or between two establishments of the Processor, or with a Sub-processor by the Processor.

    7. “**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.

    8. “**European Data Protection Laws**” means: (i) Regulation 2016/679 of the European Parliament and of the Council 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) (“**GDPR**”); (ii) Directive 2002/58/EC concerning the Processing of personal data and the protection of privacy in the electronic communications sector, as amended by Directive 2009/136/EC (“e-Privacy Directive”); (iii) any applicable national implementations of (i) and (ii); (iv) the Swiss Federal Data Protection Act of 25 September 2020 (as entered into force on 1 September 2023) and its implementing ordinances; and (v) in respect of the United Kingdom (“**UK**”), the Data Protection Act 2018 and any applicable national legislation that replaces or converts in domestic law the GDPR, e-Privacy Directive or any other law relating to data and privacy, in each case as the same may be amended, superseded or replaced.

    9. “**Personal Data**” means any information that relates to an identified or identifiable natural person and which is protected as “personal data”, “personal information” or “personally identifiable information” under Applicable Data Protection Laws.

    10. “**Process**,” “**Processes**,” “**Processing**,” “**Processed**” means any operation or set of operations which is performed on Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, destruction, or creating information from, Personal Data.

    11. “**Processor**” means a natural or legal person, public authority, agency, or other body which Processes personal data on behalf of the controller.

    12. “**Restricted Transfer**” means: (i) where the GDPR applies, a transfer of Personal Data from the EEA to a country outside of the EEA which is not subject to an adequacy determination by the European Commission ("ex-EEA"); (ii) where the UK

GDPR applies, a transfer of Personal Data from the UK to any other country which is not based on adequacy regulations pursuant to Section 17A of the Data Protection Act 2018 ("ex-UK"); and (iii) where the Swiss DPA applies, a transfer of Personal Data to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner.

13. "**Security Incident**" means a personal data breach or any confirmed breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data transmitted, stored or otherwise Processed by CodeRabbit in connection with the provision of the Services. "Security Incident" shall not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks and other network attacks on firewalls or networked systems.

14. "**Standard Contractual Clauses**" or "**SCCs**" means (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EU SCCs**"); (ii) where the UK Data Protection Law applies, either (a) the International Data Transfer Addendum to the EU SCCs issued by the UK Information Commissioner, or (b) any standard data protection clauses for Processprocessors adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR ("**UK SCCs**"); and (iii) where the Swiss DPA applies, the applicable standard data protection clauses issued, approved or recognised by the Swiss Federal Data Protection and Information Commissioner for transfers of personal data to third countries (the "**Swiss SCCs**").

15. "**Sub-processor**" means any Processor engaged by the Processor or its Affiliates to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA. Sub-processors may include third parties or Affiliates of Processor.

16. "**US Data Protection Law**" means all privacy laws and regulations applicable in the United States, including the: (i) California Consumer Privacy Act, as amended by the California Privacy Rights Act of 2020 (the "**CCPA**"); (ii) Colorado Privacy Act (the "**CPA**"); (iii) Connecticut Data Privacy Act (the "**CTDPA**"); (iv) Delaware Personal Data Privacy Act ("**DPDPA**"); (v) Iowa Consumer Data Protection Act ("**ICDPA**"); (vi) Montana Consumer Data Privacy Act ("**MCDPA**"); (vii) Nebraska Data Privacy Act ("**NDPA**"); (viii) Oregon Consumer Privacy Act ("**OCPA**"); (ix) Texas Data Privacy and Security Act ("**TDPSA**"); (x) New Hampshire Privacy Act ("**NHPA**"); (xi) New Jersey Privacy Act ("**NJPA**"); (xii) Utah Consumer Privacy Act (the "**UCPA**"); and (xiii) the Virginia Consumer Data Protection Act (the "**VCDPA**"), in each case as may be amended or superseded from time to time. The terms "controller" and "processor" include "business" and "service provider," respectively, each as defined in the CCPA.

2. **Scope and Applicability of this DPA.** This DPA applies where and only to the extent that (i) CodeRabbit Processes Customer Data on behalf of Customer as a Processor in the course of providing the Services, and (ii) this DPA is expressly incorporated by reference into the applicable Agreement between CodeRabbit and Customer. If there is a conflict between the provisions of the Agreement and this DPA, the provisions of this DPA shall prevail with respect to the subject matter hereof.

3. **Roles and Scope of Processing.**

1. **Role of the Parties.** As between CodeRabbit and Customer, CodeRabbit shall Process Customer Data only as a Processor (or Sub-processor) acting on behalf of Customer and, where applicable, as a service provider, in each case, regardless of whether Customer acts as a controller or as a data Processor on behalf of a third-party controller with respect to Customer Data.

2. **Categories of Personal Data and Data Subjects.** The Controller authorizes permission to the Processor to Process Personal Data to the extent of which is determined and regulated by the Controller. The current nature of Personal Data is specified in Annex I to this DPA.

3. **Customer Instructions.** CodeRabbit shall Process Customer Data only for the purposes described in the Agreement and in accordance with Customer's documented lawful instructions (the "**Business Purposes**"). The parties agree that the Agreement and applicable Order Form (including this DPA) sets out the Customer's complete and final instructions to CodeRabbit in relation to the Processing of Customer Data. CodeRabbit shall notify Customer in writing, unless prohibited from doing so under Applicable Data Protection Laws, if it becomes aware or believes that any data Processing instructions from Customer violate Applicable Data Protection Laws.

4. **Customer Responsibilities.** Customer is responsible for the lawfulness of Customer Data Processing under or in connection with the Services. Customer shall (i) have provided, and will continue to provide all notices and have obtained, and will continue to obtain, any applicable consents, permissions and rights necessary under Applicable Data Protection Laws for CodeRabbit to lawfully Process Customer Data for the purposes contemplated by the Agreement (including this DPA); (ii)

comply with all Applicable Data Protection Laws applicable to the collection of Customer Data and the transfer of such Customer Data to CodeRabbit and its Sub-processors; and (iii) take commercially reasonable steps designed to ensure its Processing instructions comply with applicable laws (including Applicable Data Protection Laws). Where applicable, Customer shall be responsible for any communications, notifications, assistance and/or authorizations that may be required in connection with any third-party controllers for whom Customer acts as a Processor.

5. **CodeRabbit as Controller.**

1. The parties acknowledge and agree that CodeRabbit is an independent controller, not joint controller with Customer, with respect to (a) CodeRabbit Account Data and (b) Personal Data that CodeRabbit independently collects and Processes in connection with the provision of the Services, including activity logs, communication metadata, and data used to provide, optimize, maintain, and secure the Services (together with CodeRabbit Account Data, "**CodeRabbit Controller Data**"). CodeRabbit will Process CodeRabbit Controller Data as a controller: (i) to manage the relationship with Customer; (ii) to carry out CodeRabbit'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 CodeRabbit is subject; and (vi) as otherwise permitted under Applicable Data Protection Law and in accordance with this DPA and the Agreement.

2. Each party shall be individually and separately responsible for complying with the obligations that apply to it as a separate, independent Controller under Applicable Data Protection Law and neither party shall be responsible for the other party's compliance with Applicable Data Protection Law.

4. **Security and Audits.**

1. **Security Measures**. Taking into account the state of the art, 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, CodeRabbit shall maintain appropriate technical and organizational security measures designed to protect Customer Data from Security Incidents and to preserve the security and confidentiality of Customer Data. Such measures will include, at minimum, those measures described in Annex 2 of this DPA ("**Security Measures**"). CodeRabbit shall ensure that any person who is authorized by CodeRabbit to Process Customer Data shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty). ■

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

3. **Customer Security Responsibilities.** Notwithstanding the above, Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Services, including securing its account authentication credentials, protecting the security of Customer Data when in transit to and from the Services and taking any appropriate steps to securely encrypt or backup any Customer Data Processed in connection with the Services. Customer shall maintain appropriate technical and organizational security measures designed to protect Personal Data from Security Incidents and to preserve the security and confidentiality of Personal Data while in its dominion and control.■

4. **Security Incident Response.** Upon becoming aware of a Security Incident, CodeRabbit shall notify Customer without undue delay and shall provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer. CodeRabbit will, taking into account the nature of the Processing and the information available to CodeRabbit, provide Customer with reasonable cooperation and assistance necessary for Customer to comply with its obligations under Applicable Data Protection Law with respect to notifying (i) the relevant Supervisory Authority or regulatory agency and (ii) Data Subjects affected by such Security Incident without undue delay. The obligations under this section regarding cooperation and assistance will not apply to the extent that a Security Incident results solely and directly from the actions or omissions of Customer, provided that CodeRabbit shall in all cases notify Customer of any Security Incident affecting Customer Data as set forth herein. CodeRabbit's notification of or response to a Security Incident in accordance with this section will not be construed as an acknowledgment by CodeRabbit of any fault or liability with respect to the Security Incident.■

5. **Data Protection Audits.** CodeRabbit will keep records of its Processing activities in compliance with Applicable Data Protection Law. On written request from Customer, CodeRabbit shall provide written responses (which may include audit report summaries/extracts) to all reasonable requests for information made by Customer related to its Processing of Customer

Data necessary to confirm CodeRabbit's compliance with this DPA, provided that Customer shall not exercise this right more than once in any rolling 12-month period. Notwithstanding the foregoing, Customer may also exercise such audit right in the event Customer is expressly requested or required to provide this information to a data protection authority, or CodeRabbit has experienced a Security Incident, or on another reasonably similar basis. Nothing herein shall be construed to require CodeRabbit to provide: (i) trade secrets or any proprietary information; (ii) any information that would violate CodeRabbit's confidentiality obligations, contractual obligations, or applicable law; or (iii) any information, the disclosure of which could threaten, compromise, or otherwise put at risk the security, confidentiality, or integrity of CodeRabbit's infrastructure, networks, systems, or data.

5. **Sub-processors**

1. Customer hereby provides a general authorization to CodeRabbit to engage Sub-processors to Process Customer Data on CodeRabbit's behalf (with respect to its role as a Processor). Such Sub-processor(s) shall take technical and organizational measures designed to ensure confidentiality of Customer Data shared with them. The current Sub-processors engaged by CodeRabbit are listed in Annex III hereto. CodeRabbit shall be responsible for any failure on behalf of a Sub-processor to fulfil its data protection obligations under this DPA in connection with the performance of the Services.

2. CodeRabbit shall notify Customer at least thirty (30) days in advance of any change to Annex III. If Customer has a concern that the Sub-processor(s) Processing of Customer Data is reasonably likely to cause the Controller to breach its data protection obligations under Applicable Data Protection Law, Customer may object to CodeRabbit's use of such Sub-processor (a) on reasonable grounds relating to data protection (if making Personal Data available to the proposed subprocessor would violate applicable data protection laws or weaken the protections for Customer's Personal Data) and (b) within ten (10) business days of receiving such notification, and the Parties shall confer in good faith to address such concern with a view to achieving a mutually acceptable resolution. If the parties cannot reach a mutually acceptable resolution within a reasonable time thereafter, CodeRabbit will, in its sole discretion, either (i) not appoint the subprocessor or (ii) permit Customer to suspend or terminate the Agreement. The obligations and rights under this Section 5.2 shall only apply to the extent accorded under Applicable Data Protection Law.

6. **Return and Deletion of Personal Data.** Upon termination or expiration of the Agreement, on Customer's request, CodeRabbit shall return or delete all Customer Data Processed by CodeRabbit as a Processor (including copies) in its possession or control in accordance with the Agreement, save that this requirement shall not apply to the extent CodeRabbit is required by applicable law to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems, which data CodeRabbit shall securely isolate and protect from any further Processing and delete in accordance with its deletion practices, except to the extent required by applicable law. Customer Data Processed by CodeRabbit as a Controller will be deleted or retained in accordance with the CodeRabbit Privacy Policy. Where Section 8.2 (Ex-EEA Restricted Transfers) is applicable, the parties agree that the certification of deletion of Personal Data described in the SCCs, as applicable, shall be provided by CodeRabbit to Customer only upon Customer's request.

7. **Rights of Individuals and Cooperation.** To the extent Customer is unable to independently access the relevant Customer Data within the Services, CodeRabbit shall, at Customer's expense and taking into account the nature of the Processing, provide reasonable cooperation to assist Customer to respond to any requests from individuals or applicable data protection authorities relating to the Processing of Customer Data under the Agreement. In the event that any such request is made to CodeRabbit directly, and CodeRabbit is able to readily discern that such request is associated with Customer, CodeRabbit shall not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. If CodeRabbit is required to respond to such a request, CodeRabbit shall promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

8. **International Transfer and Jurisdiction Specific Terms.**

1. **Transfer Jurisdictions.** Customer acknowledges and agrees that CodeRabbit and its Sub-processors may transfer (including conduct Restricted Transfers) and Process Customer Data to and in the United States and anywhere else in the world where CodeRabbit, its Affiliates or its Sub-processors maintain Processing operations, as more particularly described in Annex III. The parties shall ensure that such transfers are made in compliance with the requirements of Applicable Data Protection Law and this DPA. If CodeRabbit transfers Customer Data to a jurisdiction for which the European Commission has not issued an adequacy decision, CodeRabbit will ensure that appropriate safeguards have been implemented for the transfer of Customer Data in accordance with Applicable Data Protection Law.■

2. **Ex-EEA Restricted Transfers** The parties agree that when the transfer of Personal Data from Customer (as "**Data Exporter**") to CodeRabbit (as "**Data Importer**") is an ex-EEA Restricted Transfer, it shall be made pursuant to the SCCs, which are hereby incorporated by reference, and form an integral part of this DPA, as follows:

1. Module One (Controller to Controller) of the EU SCCs applies when CodeRabbit is Processing Customer Data as a controller pursuant to Section 3.5 of this DPA.

2. Module Two (Controller to Processor) of the EU SCCs applies when Customer is a controller and CodeRabbit is a processor of Customer Data pursuant to Section 3.1 of this DPA.

3. Module Three (Processor to Processor) of the EU SCCs applies when Customer is a processor acting on behalf of a third-party controller, and CodeRabbit is a processor of Customer Data pursuant to Section 3.1 of this DPA

4. The optional docking clause in Clause 7 will apply;

5. In Clause 9, Option 2 (general authorization) will apply, and the time period for prior notice of Sub-processor changes is identified in Section 5 of this DPA;

6. In Clause 11, the optional language will not apply;

7. All square brackets in Clause 13 are hereby removed;

8. In Clause 17, Option 1 will apply, and the SCCs will be governed by the law of the EU Member State in which the data exporter is established and if no such law, the laws of the Republic of Ireland;

9. In Clause 18(b), disputes shall be resolved before the courts of the law of the EU Member State in which the data exporter is established and if no such law, the laws of the Republic of Ireland;

10. Annex I of the SCCs shall be deemed completed with the information set out in Annex 1 of this DPA; and

11. Annex II of the SCCs shall be deemed completed with the information set out in Annex II to this DPA.■

3. **Ex-UK Restricted Transfers**. The parties agree that ex-UK Restricted Transfers shall be made pursuant to: (i) the Data Privacy Framework to the extent the recipient of the ex-UK Restricted Transfer is certified accordingly; or (ii) the SCCs as completed in accordance with Section 8.2 above.

4. **Restricted Transfers from Switzerland**. The parties agree that Restricted Transfers from Switzerland shall either be made pursuant to: (i) the Data Privacy Framework to the extent that recipient of the transfer from Switzerland is certified accordingly; or (ii) the SCCs with the following modifications:

1. references to “Regulation (EU) 2016/679” or specific Articles thereof shall be interpreted as references to the Swiss DPA and its equivalent sections;

2. references to “EU”, “Union”, “Member State” and “Member State law” shall be replaced with references to “Switzerland”, or “Swiss law”;

3. the term “member state” shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (i.e., Switzerland);

4. Clause 13(a) and Part C of Annex I are not used and the "competent supervisory authority" is the Swiss Federal Data Protection and Information Commissioner;

5. references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Swiss Federal Data Protection and Information Commissioner" and "applicable courts of Switzerland";

6. in Clause 17, the SCCs shall be governed by the laws of Switzerland;

7. Clause 18(b) shall state that disputes shall be resolved before the applicable courts of Switzerland; and

8. the SCCs shall also protect the data of legal entities until the entry into force of the revised Swiss Federal Data Protection Act.■■

5. ■**Supplementary Measures.** In respect of any ex-EEA, ex-UK or Switzerland-related Restricted Transfer, the following supplementary measures shall apply:

1. As of the date of this DPA, CodeRabbit has not received any formal legal requests from any government intelligence or security service/agencies in the country to which Customer Data is being exported, for access to (or for copies of) Customer Data (“**Government Agency Requests**”);

2. If, after the date of this DPA, CodeRabbit receives any Government Agency Requests, CodeRabbit shall attempt to redirect the law enforcement or government agency to request that data directly from Customer. As part of this effort,

CodeRabbit may provide Customer's basic contact information to the government agency. If compelled to disclose Customer Data to a law enforcement or government agency, CodeRabbit shall give Customer reasonable notice of the demand and cooperate to allow Customer to seek a protective order or other appropriate remedy unless CodeRabbit is legally prohibited from doing so. CodeRabbit shall not voluntarily disclose Customer Data to any law enforcement or government agency. Customer and CodeRabbit shall (as soon as reasonably practicable) discuss and determine whether all or any transfers of Customer Data pursuant to this DPA should be suspended in the light of such Government Agency Requests; and

3. Customer and CodeRabbit may meet, as reasonably requested by either Party or as required under applicable Data Protection Laws, to consider whether: (i) the protection afforded by the laws of the country where CodeRabbit is based to data subjects whose Customer 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 Applicable Data Protection Law; and (iii) it is still appropriate for Customer Data to be transferred to CodeRabbit, considering all relevant information available to the parties, along with guidance provided by Supervisory Authorities. ■

6. **Alternative Transfer Arrangement**. If, and to the extent CodeRabbit adopts an alternative data export solution (including adopting Binding Corporate Rules or any new version of or successor to the SCCs or Data Privacy Framework adopted pursuant to applicable European Data Protection Law) for the transfer of Customer Data as prescribed by applicable European Data Protection Laws ("**Alternative Transfer Mechanism**"), the Alternative Transfer Mechanism shall apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with applicable European Data Protection Law and extends to the territories to which Customer Data is transferred) and Customer agrees to execute such other and further documents and take such other and further actions as may be reasonably necessary to give legal effect such Alternative Transfer Mechanism. In addition, if and to the extent that a court of competent jurisdiction or a supervisory authority with binding authority orders (for whatever reason) that the measures described in this DPA cannot be relied on to lawfully transfer Customer Data to a country that does not ensure an adequate level of protection (within the meaning of applicable European Data Protection Law), the parties shall reasonably cooperate to agree and take any actions that may be reasonably required to implement any additional measures or safeguards not described in this DPA or alternative transfer mechanisms to enable the lawful transfer of such Customer Data.■

7. **Data Protection Impact Assessment**. To the extent CodeRabbit is required under applicable European Data Protection Law, CodeRabbit shall provide reasonably requested information regarding CodeRabbit's Processing of Customer Data under the Agreement and this DPA to enable Customer to carry out data protection impact assessments or prior consultations with Supervisory Authorities as required by law.

8. **United States Data Protection Laws**.

1. As a service provider, CodeRabbit shall not: (a) sell or share Customer Data, as these terms are defined under US Data Protection Law; (b) retain, use, or disclose Customer Data for any purpose other than for the Business Purposes, including retaining, using, or disclosing Customer Data for a commercial purpose other than the Business Purposes, or as otherwise permitted by US Data Protection Law; (c) retain, use, or disclose Customer Data outside of the direct business relationship between CodeRabbit and Customer; or (d) combine Customer Data that CodeRabbit receives from, or on behalf of, Customer with personal information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer, provided that CodeRabbit may combine personal information to perform any Business Purpose in accordance with US Data Protection Law.

2. CodeRabbit shall: (a) provide reasonable assistance to Customer where a risk assessment, cybersecurity audit or similar is required under US Data Protection Law and/or a query, inquiry, complaint or prior consultation with a Supervisory Authority is required over compliance with US Data Protection Law; (b) grant Customer the right to take reasonable and appropriate steps to help ensure that CodeRabbit uses Customer Data in a manner consistent with Customer's obligations under US Data Protection Law; (c) notify Customer if CodeRabbit determines that it can no longer meet its obligations under US Data Protection Law; (d) grant Customer the right, upon reasonable notice, to take reasonable and appropriate steps to stop and remediate any unauthorized use of Customer Data.

3. To the extent required by US Data Protection Law, Customer shall inform CodeRabbit of any consumer requests made pursuant to US Data Protection Law that CodeRabbit must comply with, and shall provide all information reasonably necessary for CodeRabbit to comply with such request.

9. **Miscellaneous**.

1. **Disclosures**. Customer acknowledges that CodeRabbit may disclose this DPA (including the Standard Contractual Clauses) and any relevant privacy provisions in the Agreement to the U.S. Department of Commerce, the Federal Trade Commission, a European data protection authority or any other U.S. or European judicial or regulatory body upon their request.■

2. **Necessary Modifications**. Notwithstanding anything to the contrary in the Agreement, CodeRabbit may modify the terms of this DPA where necessary to (i) comply with a request or order by a Supervisory Authority; (ii) comply with Applicable Data Protection Law; or (iii) implement or adhere to the Standard Contractual Clauses, approved codes of conduct or certifications, binding corporate rules, or other compliance mechanisms, which may be permitted under Applicable Data Protection Law. Supplemental terms may be added as an Annex to this DPA where such terms only apply to the Processing of Customer Data under the Applicable Data Protection Law of specific countries or jurisdictions. CodeRabbit shall provide notice of such changes to Customer, and the modified DPA shall become effective in accordance with the terms of the Agreement or, if not specified in the Agreement, as otherwise provided on CodeRabbit's website.■

3. **Conflicts**. Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict. It is not the intention of either party to contradict or restrict any of the provisions set forth in the SCCs and, accordingly, if and to the extent the SCCs conflict with any provision of the Agreement (including this DPA), the SCCs shall prevail to the extent of such conflict.■

4. **Claims**. Any claims brought under or in connection with this DPA shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement. In particular, any claim or remedy Customer or its Affiliates may have against CodeRabbit, its Affiliates, employees, contractors, agents and Sub-processors, arising under or in connection with this DPA, whether in contract, tort (including negligence) or under any other theory of liability, shall to the maximum extent permitted by law be subject to the limitations and exclusions of liability in the Agreement. Accordingly, any reference in the Agreement to the liability of a party means the aggregate liability of that party and all of its Affiliates under and in connection with the Agreement and this DPA together. Notwithstanding the foregoing, in no event may any party limit its liability with respect to any Data Subject rights or Supervisory Authorities under this DPA.■

5. **Severability**. If any provision or part-provision of this DPA is or becomes invalid, illegal or unenforceable, it shall be deemed deleted, but that shall not affect the validity and enforceability of the rest of the DPA.■

6. **Governing Law**. This DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by Applicable Data Protection Law or the SCCs.

ANNEX I

Schedule 1

(C2P / Module 2 Transfers)

A. LIST OF PARTIES

Data exporter(s):

Name: **Customer (As set forth in the relevant Order Form)**.

Address: **As set forth in the relevant Order Form.**

Contact person's name, position, and contact details: **As set forth in the relevant Order Form**.

Activities relevant to the data transferred under these Clauses: **Recipient of the Services provided by CodeRabbit Inc. in accordance with the Agreement**.

Signature and date: **Signature and date are set out in the Agreement**.

Role (Controller/ Processor): **Controller**

Data importer(s):

Name: **CodeRabbit Inc.**

Address: **201 Spear Street, 12th Floor, San Francisco CA 94105 United States**

Contact person's name, position, and contact details: **Vishavjeet Kaur, dpo@coderabbit.ai , +1 - 888 - 247 - 5357**

Activities relevant to the data transferred under these Clauses: **Provision of the Services to the Customer in accordance with the Agreement**.

Signature and date: **Signature and date are set out in the Agreement**.

Role (controller/processor): **Processor**.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Authorized users of the Services. Users, as this term is defined in the Terms of Service and Master Services Agreement, as applicable.

Categories of personal data transferred

Git platform (GitHub, GitLab, AzureDevOps, Bitbucket) User ID, Username, User's primary email.

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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

No sensitive data collected.

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

Continuous basis

Nature of the Processing

The data importer's Processing activities shall be limited to those set forth in the Agreement and the DPA.

Purpose(s) of the data transfer and further Processing

The purpose of the transfer is to facilitate the performance of the Services more fully described in the Agreement and accompanying order forms.

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

The period for which the Customer Data will be retained is more fully described in the Agreement, Addendum, and accompanying Order Forms.

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

The subject matter, nature, and duration of the Processing more fully described in the Agreement, Addendum, and accompanying order forms.

C.COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority will be determined in accordance with European Data Protection Law.

Schedule 2

(C2C / Module 1 Transfers)

A. LIST OF PARTIES

Data exporter(s):

Name: **Customer (As set forth in the relevant Order Form)**.

Address: **As set forth in the relevant Order Form.**

Contact person's name, position, and contact details: **As set forth in the relevant Order Form**.

Activities relevant to the data transferred under these Clauses: **Recipient of the Services provided by CodeRabbit Inc. in accordance with the Agreement**.

Signature and date: **Signature and date are set out in the Agreement**.

Role (Controller/ Processor): **Controller**

Data importer(s):

Name: **CodeRabbit Inc.**

Address: **201 Spear Street, 12th Floor, San Francisco CA 94105 United States**

Contact person's name, position, and contact details: **Vishavjeet Kaur, dpo@coderabbit.ai , +1 - 888 - 247 - 5357**

Activities relevant to the data transferred under these Clauses: **Provision of the Services to the Customer in accordance with the Agreement**.

Signature and date: **Signature and date are set out in the Agreement**.

Role (Controller/Processor): **Controller**.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Authorized users of the Services. Users, as this term is defined in the Terms of Service and Master Services Agreement, as applicable.

Categories of personal data transferred

CodeRabbit Account Data and CodeRabbit Usage Data

Service operational data collected by CodeRabbit as controller, including activity logs, communication metadata (source and destination identifiers), and performance and security telemetry collected in connection with the provision of the Services.

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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

No sensitive data collected.

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

Continuous basis, dependent on Customer's use of the Services

Nature of the Processing

The data importer's Processing activities shall be limited to those discussed in the Agreement and the DPA

Purpose(s) of the data transfer and further Processing

CodeRabbit will Process the Personal Data for the following business purposes: (i) account registration, (ii) order and purchase, (iii) customer communications and support, (iv) to operate and enhance CodeRabbit offerings; (v) to prevent, detect and investigate security incidents; and (vi) to resist and respond to malicious, deceptive, fraudulent or illegal actions.

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

The period for which the Customer Data will be retained is more fully described in the Agreement, Addendum, and accompanying order forms.

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

The subject matter, nature, and duration of the Processing more fully described in the Agreement, Addendum, and accompanying order forms.

C.COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority will be determined in accordance with European Data Protection Law.

Schedule 3

(P2P / Module 3 Transfers)

A. LIST OF PARTIES

Data exporter(s):

Name: **Customer (As set forth in the relevant Order Form).**

Address: **As set forth in the relevant Order Form.**

Contact person's name, position, and contact details: **As set forth in the relevant Order Form.**

Activities relevant to the data transferred under these Clauses: **Recipient of the Services provided by CodeRabbit Inc. in accordance with the Agreement.**

Signature and date: **Signature and date are set out in the Agreement.**

Role (Controller/ Processor): **Processor**

Data importer(s):

Name: **CodeRabbit Inc.**

Address: **201 Spear Street, 12th Floor, San Francisco CA 94105 United States**

Contact person's name, position, and contact details: **Vishavjeet Kaur, dpo@coderabbit.ai, +1 - 888 - 247 - 5357**

Activities relevant to the data transferred under these Clauses: **Provision of the Services to the Customer in accordance with the Agreement.**

Signature and date: **Signature and date are set out in the Agreement.**

Role (controller/processor): **Processor.**

B. DESCRIPTION OF TRANSFER

Categories of data subjects transferred:

Authorized users of the Services. Users, as this term is defined in the Terms of Service and Master Services Agreement, as applicable.

Categories of personal data transferred:

Git platform (GitHub, GitLab, AzureDevOps, Bitbucket) User ID, Username, User's primary email.

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 log of access to the data, restrictions for onward transfers or additional security measures:

No sensitive data collected.

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

Continuous basis

Nature of the processing

The data importer's Processing activities shall be limited to those set forth in the Agreement and the DPA.

Purpose(s) of the data transfer and further processing:

The purpose of the transfer is to facilitate the performance of the Services more fully described in the Agreement and accompanying order forms.

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

The period for which the Customer Data will be retained is more fully described in the Agreement, Addendum, and accompanying Order Forms.

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

The subject matter, nature, and duration of the Processing more fully described in the Agreement, Addendum, and accompanying order forms.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority will be determined in accordance with European Data Protection Law.

ANNEX II

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

Description of the technical and organisational security measures implemented by CodeRabbit Inc. as the data Processor/data importer to ensure an appropriate level of security, taking into account the nature, scope, context, and purpose of the Processing, and the risks for the rights and freedoms of natural persons.

Security

Security Management System.

Organization. CodeRabbit Inc. designates qualified security personnel whose responsibilities include development, implementation, and ongoing maintenance of the Information Security Program.

Policies. Management reviews and supports all security related policies to ensure the security, availability, integrity and confidentiality of Customer Data. These policies are updated at least once annually.

Assessments. CodeRabbit Inc. engages a reputable independent third-party to perform risk assessments of all systems containing Customer Data at least once annually.

Risk Treatment. CodeRabbit Inc. maintains a formal and effective risk treatment program that includes penetration testing, vulnerability management and patch management to identify and protect against potential threats to the security, integrity or confidentiality of Customer Data.

Vendor Management. CodeRabbit Inc. maintains an effective vendor management program

Incident Management. CodeRabbit Inc. reviews security incidents regularly, including effective determination of root cause and corrective action.

Standards. CodeRabbit Inc. operates an information security management system that complies with the requirements of ISO/IEC 27001:2022 standard.

Personnel Security.

CodeRabbit Inc. personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. CodeRabbit Inc. conducts reasonably appropriate background checks on any employees who will have access to client data under this Agreement, including in relation to employment history and criminal records, to the extent legally permissible and in accordance with applicable local labor law, customary practice and statutory regulations.

Personnel are required to execute a confidentiality agreement in writing at the time of hire and to protect Customer Data at all times. Personnel must acknowledge receipt of, and compliance with, CodeRabbit Inc's confidentiality, privacy and security policies. Personnel are provided with privacy and security training on how to implement and comply with the Information Security Program. Personnel handling Customer Data are required to complete additional requirements appropriate to their role (e.g., certifications).

CodeRabbit Inc's personnel will not Process Customer Data without authorization.

Access Controls

Access Management. CodeRabbit Inc. maintains a formal access management process for the request, review, approval and provisioning of all personnel with access to Customer Data to limit access to Customer Data and systems storing, accessing or transmitting Customer Data to properly authorized persons having a need for such access. Access reviews are conducted periodically to ensure that only those personnel with access to Customer Data still require it.

Infrastructure Security Personnel. CodeRabbit Inc. has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. CodeRabbit Inc's infrastructure security personnel are responsible for the ongoing monitoring of CodeRabbit Inc's security infrastructure, the review of the Services, and for responding to security incidents.

Access Control and Privilege Management. CodeRabbit Inc's and Customer's administrators and end users must authenticate themselves via a Multi-Factor authentication system or via a single sign on system in order to use the Services

Internal Data Access Processes and Policies – Access Policy. CodeRabbit Inc's internal data access processes and policies are designed to protect against unauthorized access, use, disclosure, alteration or destruction of Customer Data. CodeRabbit Inc. designs its systems to only allow authorized persons to access data they are authorized to access based on principles of "least privileged" and "need to know", and to prevent others who should not have access from obtaining access. CodeRabbit Inc. requires the use of unique user IDs, strong passwords, two factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; a need to know basis; and must be in accordance with CodeRabbit Inc's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g., login to workstations), password policies follow industry standard practices. These standards include password complexity, password expiry, password lockout, restrictions on password reuse and re-prompt for password after a period of inactivity

Data Center and Network Security

Data Centers.

Infrastructure. CodeRabbit Inc. has GCP as its data center.

Resiliency. Multi Availability Zones are enabled on GCP and CodeRabbit Inc. conducts Backup Restoration Testing on regular basis to ensure resiliency.

Server Operating Systems. CodeRabbit Inc's servers are customized for the application environment and the servers have been hardened for the security of the Services. CodeRabbit Inc. employs a code review process to increase the security of the code used to provide the Services and enhance the security products in production environments.

Disaster Recovery. CodeRabbit Inc. replicates data over multiple systems to help to protect against accidental destruction or loss. CodeRabbit Inc. has designed and regularly plans and tests its disaster recovery programs.

Security Logs. CodeRabbit Inc's systems have logging enabled to their respective system log facility in order to support the security audits, and monitor and detect actual and attempted attacks on, or intrusions into, CodeRabbit Inc's systems.

Vulnerability Management. CodeRabbit Inc. performs regular vulnerability scans on all infrastructure components of its production and development environment. Vulnerabilities are remediated on a risk basis, with Critical, High and Medium security patches for all components installed as soon as commercially possible.

Networks and Transmission.

Data Transmission. Transmissions on production environment are transmitted via Internet standard protocols.

External Attack Surface. GCP Security Group which is equivalent to virtual firewall is in place for Production environment on GCP.

Incident Response. CodeRabbit Inc. maintains incident management policies and procedures, including detailed security incident escalation procedures. CodeRabbit Inc. monitors a variety of communication channels for security incidents, and CodeRabbit Inc's security personnel will react promptly to suspected or known incidents, mitigate harmful effects of such security incidents, and document such security incidents and their outcomes.

Encryption Technologies. CodeRabbit Inc. makes HTTPS encryption (also referred to as SSL or TLS) available for data in transit.

Data Storage, Isolation, Authentication, and Destruction. CodeRabbit Inc. stores data in a multi-tenant environment on GCP servers. Data, the Services database and file system architecture are replicated between multiple availability zones on GCP. CodeRabbit Inc. logically isolates the data of different customers. A central authentication system is used across all Services to increase uniform security of data. CodeRabbit Inc. ensures secure disposal of Client Data through the use of a series of data destruction processes.

ANNEX III - LIST OF SUB-PROCESSORS

https://trust.coderabbit.ai/subprocessors