SecureChain Portal Data Processing Addendum

Version 1.0
Effective date: October 15, 2026

This SecureChain Portal Data Processing Addendum ("DPA") forms part of the SecureChain Portal Terms of Use, the SecureChain Portal License Agreement, and any Order or other written or electronic agreement, by and between TuxCare, Inc. ("TuxCare") and the customer of TuxCare that accepts the Main Agreement ("Customer") for the SecureChain Portal, the related CLI and submission workflows (collectively, the "Service") (the "Main Agreement"). All capitalized terms not defined herein have the meanings set forth in the Main Agreement. Each of Customer and TuxCare may be referred to herein as a "Party" and together as the "Parties."

In connection with the Service, the Parties anticipate that TuxCare may process outside of the European Economic Area ("EEA"), Switzerland, and the United Kingdom ("UK") certain Personal Data in respect of which the Customer may be a data controller or data processor, as applicable, under Applicable Data Protection Laws.

The Parties have agreed to enter into this DPA in order to ensure that adequate safeguards are put in place with respect to the protection of such Personal Data as required by Applicable Data Protection Laws.

In the course of providing the Service to Customer pursuant to the Main Agreement, TuxCare may Process Personal Data on behalf of Customer. TuxCare agrees to comply with the following provisions with respect to any Personal Data submitted by or for Customer to TuxCare or collected and processed by or for Customer using the Service.

1. DEFINITIONS

"Applicable Data Protection Laws" means all applicable data protection, data privacy, and cybersecurity laws, rules, and regulations anywhere in the world that are in force from time to time, including but not limited to (i) the EU General Data Protection Regulation 2016/679, (ii) the Swiss Federal Act on Data Protection of 25 September 2020, in force since 1 September 2023 ("FADP"), and (iii) in respect of the United Kingdom, the GDPR as it forms part of UK law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 and the Data Protection Act 2018.

"Customer Data" means data that Customer or its users submit to the Service, including to a Workspace or through the CLI, and data the Service derives from it, as further defined in the SecureChain Portal Terms of Use and the SecureChain Portal License Agreement.

"Customer Personal Data" means Personal Data contained in Customer Data that TuxCare processes on behalf of Customer.

"Data Privacy Framework" means the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework self-certification program operated by the US Department of Commerce.

"Documented Instructions" has the meaning given in clause 2.12.

"GDPR" means the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data).

"Personal Data" means any information relating to an identified or identifiable natural person that relates to, describes, is capable of being associated with, or could be linked, directly or indirectly, with a particular natural person, as defined by Applicable Data Protection Laws, and

accessed, stored or otherwise processed by TuxCare as part of its provision of the Service to Customer.

"processing", **"data controller"**, **"data subject"**, **"supervisory authority"**, and **"data processor"** have the meanings described by the Applicable Data Protection Laws.

"Restricted Transfer" means: (i) where the GDPR applies, a transfer of Personal Data via the Service from the EEA, either directly or via onward transfer, to any country or recipient outside of the EEA not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of Personal Data via the Service from the United Kingdom, either directly or via onward transfer, to any country or recipient outside of the UK not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and (iii) a transfer of Personal Data via the Service from Switzerland, either directly or via onward transfer, to any country or recipient outside of the EEA and/or Switzerland not subject to an adequacy determination by the European Commission.

"SCC" means: (i) where the 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 ("EU SCCs"); (ii) where the UK GDPR applies, the standard data protection clauses adopted ("UK SCCs"); and (iii) where Personal Data is transferred from Switzerland to outside of Switzerland or the EEA, the EU SCCs as amended in accordance with guidance from the Swiss Data Protection Authority ("Swiss SCCs").

"Sub-processor" means any third party engaged by TuxCare to process Customer Personal Data on TuxCare's behalf in connection with the provision of the Service, including any third party engaged by such a Sub-processor.

"UK Addendum" means the International Data Transfer Addendum to the EU SCCs, a legal instrument developed by the UK's Information Commissioner's Office (ICO).

"US State Privacy Laws" means all state laws relating to the protection and processing of Personal Data in effect in the United States of America, which may include, without limitation, the California Consumer Privacy Act as amended by the California Privacy Rights Act and its implementing regulations ("CCPA"), the Colorado Privacy Act, the Connecticut Data Privacy Act, and the Delaware Personal Data Privacy Act.

For the purposes of clause 7, "Service Provider", "Processor", "sell" and "share" have the meanings given in the US State Privacy Laws.

2. STATUS OF THE PARTIES

2.1 The type of Personal Data processed pursuant to this DPA and the subject matter, duration, nature, and purpose of the processing, and the categories of data subjects, are as described in Annex 1.

2.2 Each Party warrants in relation to Personal Data that it will comply (and will procure that any of its personnel comply and use commercially reasonable efforts to procure that its Sub-processors comply) with Applicable Data Protection Laws. As between the Parties, the Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which the Customer acquired Personal Data.

2.3 In respect of Customer Personal Data, the Parties acknowledge and agree that the Customer is the controller (or, where the Customer acts on behalf of another controller, the processor), and TuxCare is the processor (or sub-processor), as applicable. TuxCare shall process Customer Personal Data only in accordance with this DPA.

2.3.1 This DPA applies to Personal Data within Customer Data that TuxCare processes under Customer's instructions. TuxCare acts as an independent controller for its own account administration, access security, billing, and business communications. The SecureChain Portal Privacy Policy describes that controller processing. Contract acceptance does not supply consent from every person named in a repository or SBOM.

2.4 If Customer is an EU-based data processor, Customer warrants to TuxCare that Customer's instructions and actions with respect to the Personal Data, including its appointment of TuxCare as another processor and concluding the SCC with all relevant Appendices, have been authorized by the relevant controller. If Customer is a UK-based data processor, Customer warrants to TuxCare that Customer's instructions and actions with respect to the Personal Data, including its appointment of TuxCare as another processor and concluding the UK Addendum, have been authorized by the relevant controller. If Customer is a Swiss-based data processor, Customer warrants to TuxCare that Customer's instructions and actions with respect to the Personal Data, including its appointment of TuxCare as another processor and entering into the SCC required for international data transfers in compliance with the Swiss FADP, have been authorized by the relevant controller.

2.5 Each Party shall appoint a Data Privacy Officer within its organization authorized to respond from time to time to inquiries regarding Personal Data; the Parties shall make the Data Privacy Officer known to the other Party, and the Data Privacy Officer shall deal with such inquiries promptly.

2.6 Throughout the term of the Main Agreement, the Customer continuously guarantees that all Personal Data provided to TuxCare has been lawfully collected and transferred in full compliance with Applicable Data Protection Laws. During this DPA's term, the Customer is solely responsible for ensuring that it has, and maintains, a valid lawful basis under Applicable Data Protection Laws (including consent where consent is required) for TuxCare's processing of Customer Personal Data under the Main Agreement and this DPA, and for obtaining and maintaining all necessary authorizations from the relevant data subjects.

2.7 Customer warrants that it has provided all necessary information and notices to data subjects regarding the processing of their Personal Data, including the engagement of TuxCare, in a manner that is transparent, intelligible, and easily accessible. This includes individuals whose Personal Data appears in Customer Data without being Customer's personnel, such as upstream package authors, supplier contacts and commit authors. This clause 2.7 applies only to Personal Data that the Customer provides or makes available to TuxCare or instructs TuxCare to collect.

2.8 Customer warrants that the Personal Data provided to TuxCare is accurate and, where necessary, kept up to date. Customer will instruct TuxCare of any corrections or erasures required to maintain the accuracy of the data.

2.9 Customer warrants that the scope of Personal Data disclosed is limited to what is adequate, relevant, and necessary in relation to the purposes for which it is processed as specified in this DPA.

2.10 Customer warrants that its instructions to TuxCare for the processing of Personal Data shall at all times be lawful and in compliance with Applicable Data Protection Laws.

2.11 Customer is solely responsible for determining whether the security measures implemented within the Service are adequate to meet its obligations under Applicable Data Protection Laws. The Customer is also responsible for ensuring the secure use of the Service, including the protection of Personal Data transmitted to and from the Service.

2.12 Documented Instructions. The Parties agree that this DPA, the Main Agreement, the Documentation, and Customer's use and configuration of the Service in accordance with the Main Agreement constitute Customer's complete documented instructions to TuxCare for the processing of Customer Personal Data. By submitting an inventory, dependency report or SBOM to a Workspace, Customer instructs TuxCare to store it, match it against advisory and catalogue data, re-evaluate it against advisories published later for as long as it is retained, compare it with earlier and later submissions, generate findings and recommendations, and send alerts to the destinations Customer has configured. Additional instructions during the term must be consistent with the Main Agreement and the nature of the Service and take effect when TuxCare confirms them in writing.

3. TUXCARE OBLIGATIONS

3.1 With respect to all Personal Data, TuxCare warrants that it shall:

(a) only process Personal Data in order to provide the Service, and shall act only in accordance with (i) this DPA, (ii) the Customer's written instructions as set forth in the Main Agreement and this DPA, and (iii) as required by Applicable Data Protection Laws;

(b) immediately inform Customer if, in TuxCare's opinion, a Documented Instruction infringes Applicable Data Protection Laws, and TuxCare may suspend performance of that instruction until Customer confirms, modifies or withdraws it. TuxCare is not obliged to perform a legal review of Customer's instructions;

(c) implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks presented by the processing of Personal Data, in particular protection against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data. Such measures include, without limitation, the security measures commonly adopted in accordance with recognized security standards, such as SOC 2 Type II or ISO 27001, and as required by Applicable Data Protection Laws;

(d) take reasonable steps to ensure that only authorized personnel have access to such Personal Data and that any persons whom it authorizes to have access to the Personal Data are under obligations of confidentiality;

(e) without undue delay after becoming aware, and in any event within twenty-four (24) hours of becoming aware, notify the Customer of any 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 TuxCare, its sub-processors, or any other identified or unidentified third party (a "Security Breach"). The initial notification shall contain the facts then reasonably available to TuxCare, and TuxCare shall provide supplemental information as its investigation develops and in any event within seventy-two (72) hours of becoming aware;

(f) promptly provide the Customer with reasonable cooperation and assistance in respect of a Security Breach and all reasonable information in TuxCare's possession concerning such Security Breach insofar as it affects the Customer, including, to the extent then known: the possible cause and consequences for the data subjects of the Security Breach; the categories of Personal Data involved; a summary of the possible consequences for the relevant data subjects; a summary of the unauthorized recipients of the Personal Data; and the measures taken by TuxCare to mitigate any damage;

(g) not make any public announcement about a Security Breach (a "Breach Notice") without the prior written consent of the Customer, unless required by Applicable Data Protection Laws. This does not prevent TuxCare from publishing a general notice about a Security Breach affecting multiple customers that does not identify Customer or Customer Personal Data;

(h) promptly notify the Customer if it receives a request from a data subject of Customer to access, rectify, or erase that individual's Personal Data, or if a data subject objects to the processing of, or makes a data portability request in respect of, such Personal Data (each a "Data Subject Request"). TuxCare shall not respond to a Data Subject Request without the Customer's prior written consent except to confirm that such request relates to the Customer, to which the Customer hereby agrees. To the extent that the Customer does not have the ability to address a Data Subject Request, then upon the Customer's request, TuxCare shall provide reasonable assistance to the Customer to facilitate such Data Subject Request to the extent able and in line with Applicable Data Protection Laws. To the extent the Customer does not respond, TuxCare may respond to the Data Subject Request in any manner it deems appropriate. Customer shall cover all reasonable costs incurred by TuxCare in connection with its provision of such assistance or response;

(i) following termination, expiry, or completion of the Service, return or delete Customer Personal Data according to Customer's instructions, including copies, unless applicable law requires retention. Deletion takes place within the periods stated in Annex 1(h), and deletion from backup copies may be delayed until those copies are overwritten in TuxCare's standard backup cycle. During that period, TuxCare restricts processing to storage, security, lawful retention, and authorized return or deletion. A restored backup remains subject to the deletion instruction. Annex 1 describes the retention arrangements;

(j) taking into account the nature of processing and the information available to TuxCare, provide such assistance to the Customer as the Customer reasonably requests in relation to TuxCare's obligations under the Applicable Data Protection Laws with respect to (i) data protection impact assessments, (ii) notifications to the supervisory authority under the Applicable Data Protection Laws and/or communications to data subjects by the Customer in response to any Security Breach, and (iii) the Customer's compliance with its obligations under the Applicable Data Protection Laws with respect to the security of processing, provided that the Customer shall cover all reasonable costs incurred by TuxCare in connection with its provision of such assistance;

(k) provide to the Customer information about the region and country where the Personal Data is stored and processed by or on behalf of TuxCare;

(l) communicate the exact address of the relevant facilities only in the event of an explicit request of a competent supervisory authority and if that communication is suitable to discharge its obligation under Applicable Data Protection Laws;

(m) maintain a record of all categories of processing activities carried out on behalf of the Customer in accordance with Article 30(2) GDPR and make it available to the supervisory authority on request; and

(n) cooperate, on request, with the competent supervisory authority in the performance of its tasks.

3.2 TuxCare shall not process Customer Personal Data for its own purposes. Any processing by TuxCare of data derived from the Service for its own purposes is limited to the processing described in clause 2.3.1 as falling outside this DPA and is disclosed in the SecureChain Portal Privacy Policy.

3.3 If TuxCare receives a legally binding request from a public authority for disclosure of Customer Personal Data, TuxCare shall (a) where possible, redirect the authority to Customer; (b) promptly notify Customer unless legally prohibited from doing so; (c) review the legality of the request and challenge it where there are reasonable grounds to consider it unlawful under the law applicable to TuxCare; and (d) disclose only the minimum amount of information required.

TuxCare shall not disclose Customer Personal Data to a public authority on a voluntary basis. This clause applies irrespective of whether the processing involves a Restricted Transfer.

4. SUB-PROCESSING

4.1 The Customer grants TuxCare a general written authorization to engage Sub-processors for the provision of the Service. The Sub-processors engaged at the Effective Date are listed in Annex 3, which states for each Sub-processor its name, location, the processing it performs, and the transfer mechanism relied on. Sub-processors are engaged only for hosting, storage and backup, notification delivery, monitoring, support tooling and other functions necessary to provide the Service.

4.2 TuxCare shall notify Customer of any intended addition or replacement of a Sub-processor in accordance with clause 4.4. Customer may object on reasonable grounds relating to data protection by written notice to privacy@tuxcare.com within thirty (30) days of the notice. The Parties shall discuss the objection in good faith. If the Parties do not resolve the objection within thirty (30) days of Customer's notice, Customer may, as its sole remedy, terminate the affected Subscription or delete the affected Workspace, and TuxCare shall refund any prepaid fees attributable to the unused portion of the Subscription term. If Customer does not object within the period above, Customer is deemed to have authorized the Sub-processor.

4.3 TuxCare shall engage each Sub-processor under a written contract that imposes on the Sub-processor the same data protection obligations as those imposed on TuxCare in this DPA. Where a Sub-processor fails to fulfill its data protection obligations, TuxCare remains fully liable to the Customer for the performance of that Sub-processor's obligations. TuxCare shall, on request, provide the Customer with a copy of the data protection terms of its Sub-processor contracts, redacted to remove commercial information.

4.4 TuxCare will provide notice of the addition or replacement of a Sub-processor at least thirty (30) days before that Sub-processor begins processing Customer Personal Data.

5. AUDIT AND RECORDS

5.1 TuxCare shall, in accordance with Applicable Data Protection Laws, make available to the Customer such information in TuxCare's possession or control as the Customer may reasonably request with a view to demonstrating TuxCare's compliance with the obligations of data processors under Applicable Data Protection Laws in relation to its processing of Customer Personal Data.

5.2 The Customer may exercise its right of audit under Applicable Data Protection Laws in relation to Customer Personal Data through TuxCare providing:

(a) an audit report not older than eighteen (18) months, prepared by an independent external auditor, demonstrating that TuxCare's technical and organizational measures are sufficient and in accordance with an accepted industry audit standard, where such a report is available, and TuxCare's security documentation and written responses to the Customer's reasonable security questionnaire, provided not more than once in any twelve (12) month period;

(b) additional information in TuxCare's possession or control to the supervisory authority when it requests or requires additional information in relation to the processing of Customer Personal Data carried out by TuxCare under this DPA; and

(c) where the Customer requires an audit beyond the materials described in (a) and (b), such audit shall be conducted no more than once in any twelve (12) month period, on reasonable

prior written notice, during normal business hours, and in a manner that does not disrupt TuxCare's operations. The Customer shall cover the reasonable costs incurred by TuxCare in connection with any such audit.

6. DATA TRANSFERS

6.1 Primary Mechanism — Data Privacy Framework. TuxCare, Inc. participates in and certifies its compliance with the Data Privacy Framework. For so long as that certification is active and covers the Personal Data in question, TuxCare relies on the Data Privacy Framework to receive Personal Data transferred from the EEA, the United Kingdom and Switzerland to the United States, and will provide at least the same level of protection to that data as is required by the Data Privacy Framework Principles.

6.2 Fallback Mechanism — Standard Contractual Clauses. Where the Data Privacy Framework does not cover a transfer, ceases to be a valid transfer mechanism, or is suspended, invalidated or withdrawn, the EU SCCs shall apply automatically to Restricted Transfers from the EEA without further action by either Party. The EU SCCs are deemed entered into and incorporated into this DPA by reference, and are completed as follows:

(a) Customer is the "data exporter", and TuxCare is the "data importer";

(b) Module Two (Controller to Processor) applies where the Customer is a controller of Customer Personal Data, and TuxCare is a processor. Module Three (Processor to Processor) applies where the Customer is a processor acting on behalf of another controller or processor, and TuxCare is a sub-processor;

(c) in Clause 7, the optional docking clause applies;

(d) in Clause 9, Option 2 (general written authorization) applies, and the period for prior notice of Sub-processor changes is thirty (30) days, as set out in clause 4.4 of this DPA;

(e) in Clause 11, the optional language does not apply;

(f) in Clause 13, the competent supervisory authority is determined in accordance with that Clause;

(g) in Clause 17, Option 1 applies, and the EU SCCs are governed by the law of the Netherlands;

(h) in Clause 18(b), disputes are resolved by the courts of the Netherlands;

(i) Annex I of the EU SCCs is completed with the information set out in Annex 1 of this DPA. For the purposes of Annex I.A, the data exporter is the Customer as identified on acceptance of the Main Agreement or in the Order, and the data importer is TuxCare, Inc., 20791 Three Oaks Pkwy, #980, Estero, FL 33929, USA (privacy@tuxcare.com). Acceptance of the Main Agreement constitutes signature of Annex I;

(j) Annex II of the EU SCCs is completed with clause 3.1(c) and Annex 2 of this DPA; and

(k) Annex III of the EU SCCs is completed with the Sub-processor list in Annex 3.

6.3 United Kingdom. In relation to transfers of Personal Data subject to the UK GDPR, the EU SCCs (i) apply as completed in accordance with clause 6.2 above, and (ii) are deemed amended as specified by the UK Addendum, which is deemed executed by the Parties and forms an integral part of this DPA. Tables 1 to 3 in Part 1 of the UK Addendum are deemed completed with the information set out in this DPA and in Annex 1 and clauses 3.1(c) and 4. Table 4 in Part 1 is deemed completed by selecting "neither party". Any conflict between the EU SCCs and the UK Addendum is resolved in accordance with Sections 10 and 11 of the UK Addendum.

6.4 Switzerland. In relation to transfers of Personal Data protected by the Swiss FADP, the EU SCCs (i) apply as completed in accordance with clause 6.2, and (ii) are deemed amended as follows: references to "Regulation (EU) 2016/679" are interpreted as references to the Swiss FADP; in Clause 13 the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner; in Clause 17 the EU SCCs are governed by the laws of Switzerland; in Clause 18(b) disputes are resolved before the courts of Switzerland; references to member states are interpreted to include Switzerland; and data subjects in Switzerland are not excluded from enforcing their rights in their place of habitual residence in accordance with Clause 18(c).

6.5 Onward Transfers by Sub-processors. If TuxCare transfers Personal Data to a Sub-processor located outside the EEA, the UK or Switzerland, TuxCare shall ensure in advance of that transfer that a valid transfer mechanism is in place, being either the Sub-processor's own active Data Privacy Framework certification or SCCs (together with the UK Addendum or the Swiss amendments where applicable) executed for the benefit of the Customer. TuxCare has assessed, and keeps under review, the laws and practices of each country outside the EEA, the UK and Switzerland to which Customer Personal Data is transferred, as required by Clause 14 of the EU SCCs, and provides a summary of that assessment to the Customer on request.

6.6 Audit and Sub-processing under the SCCs. The Customer may exercise its audit right under Clause 8.9 of the EU SCCs as set out in, and subject to the requirements of, clause 5.2 of this DPA. TuxCare may appoint Sub-processors as set out in, and subject to the requirements of, clauses 4 and 6.5 of this DPA.

6.7 Alternative Mechanisms. If TuxCare is required to adopt an alternative transfer mechanism under Applicable Data Protection Laws, that mechanism will apply automatically in place of the mechanisms described above to the extent it complies with Applicable Data Protection Laws, and the Customer agrees to execute such documents or take such action as may reasonably be necessary to give it legal effect.

7. ADDITIONAL PROVISIONS UNDER US STATE PRIVACY LAWS

7.1 The following terms apply where TuxCare processes Personal Data subject to US State Privacy Laws. To the extent Customer Personal Data includes personal information protected under US State Privacy Laws that TuxCare processes as a Service Provider or Processor on behalf of Customer, TuxCare will process such Customer Personal Data in accordance with the US State Privacy Laws, including by complying with applicable sections of the US State Privacy Laws and providing the same level of privacy protection as required by US State Privacy Laws, and in accordance with Customer's written instructions, as necessary for the limited and specified purposes identified in this DPA. TuxCare will not:

(a) retain, use, disclose, or otherwise process such Customer Personal Data for a commercial purpose other than for the limited and specified purposes identified in this DPA, the Main Agreement, or as otherwise permitted under US State Privacy Laws;

(b) "sell" or "share" such Customer Personal Data within the meaning of the US State Privacy Laws; or

(c) retain, use, disclose, or otherwise process such Customer Personal Data outside the direct business relationship with Customer, or combine such Customer Personal Data with personal information that it receives from other sources, except as permitted under US State Privacy Laws.

7.2 TuxCare will implement measures designed to maintain the security of Personal Data, ensuring a level of privacy protection consistent with the requirements of US State Privacy Laws.

7.3 TuxCare will provide reasonable access to information necessary for the Customer to verify TuxCare's compliance with this DPA.

7.4 The Parties acknowledge and agree that the exchange of Personal Data between the Parties does not form part of any monetary or other valuable consideration exchanged between the Parties with respect to the Main Agreement or this DPA.

8. GENERAL

8.1 This DPA is without prejudice to the rights and obligations of the Parties under the Main Agreement, which shall continue to have full force and effect. In the event of any conflict between the terms of this DPA and the terms of the Main Agreement, the terms of this DPA shall prevail so far as the subject matter concerns the processing of Personal Data.

8.2 TuxCare's liability under or in connection with this DPA is subject to the limitations on liability contained in the Main Agreement. Nothing in these DPA limits or excludes any liability that cannot be limited or excluded under applicable law.

8.3 This DPA does not confer any third-party beneficiary rights; it is intended for the benefit of the Parties hereto and their respective permitted successors and assigns only, and is not for the benefit of, nor may any provision hereof be enforced by, any other person, save that this clause does not limit the third-party beneficiary rights conferred on data subjects under the SCCs.

8.4 This DPA and any action related thereto shall be governed by and construed in accordance with the laws of the State of Delaware, without giving effect to any conflict-of-laws principles, save where the SCCs provide otherwise. The Parties consent to the personal jurisdiction of, and venue in, the courts of Delaware.

8.5 This DPA is the final, complete, and exclusive agreement of the Parties with respect to the subject matter hereof and supersedes and merges all prior discussions and agreements between the Parties with respect to such subject matter. Other than in respect of statements made fraudulently, no other representations or terms shall apply or form part of this DPA. No modification of, amendment to, or waiver of any rights under this DPA will be effective unless agreed in writing, which includes the Customer's electronic acceptance of an updated version of this DPA in the same manner as the Main Agreement. This DPA may be executed in counterparts, each of which shall be deemed to be original, but all of which, taken together, shall constitute one and the same agreement. Where this DPA is executed separately, each person signing it represents and warrants that he or she is duly authorized and has the legal capacity to execute and deliver this DPA. Each Party represents and warrants to the other that the execution and delivery of this DPA and the performance of such Party's obligations hereunder have been duly authorized and that this DPA is a valid and legally binding agreement on each such Party, enforceable in accordance with its terms.

These DPA forms part of the Main Agreement and is accepted by the Customer in the same manner as the Main Agreement. No separate signature is required for this DPA to take effect. Where a Customer requires a separately executed copy of this DPA, TuxCare will provide one on request.

ANNEX 1 – DETAILS OF PERSONAL DATA AND PROCESSING ACTIVITIES

(a) The nature of Personal Data processing is subject to the following, to the extent permitted under Applicable Data Protection Laws and the Main Agreement:

- Receiving data, including collection, accessing, and recording;
- Holding data, including storage, organization, and structuring;
- Using data, including analyzing, consulting, and testing;
- Protecting data, including restricting;
- Erasing data, including destruction and deletion.

(b) The purpose is to provide the Service in accordance with the Documented Instructions. It includes storing inventories and raw submissions, matching advisories, re-evaluating retained scans against advisories published later, comparing scans, and storing findings and triage records. It also includes configured notifications, authorized image scans, support, service security, and data export or deletion. TuxCare does not publish or sell nonpublic Customer Data, use it in advertising, or train a general-purpose AI model with it without the Customer's separate authorization.

(c) Customer Personal Data can include the following, to the extent Customer submits it or instructs TuxCare to collect it:

- Identifiers in repository URLs, branch names, commit metadata, project labels, package coordinates, and relative paths.
- Names, business contact details, and other identifiers within SBOM authors, suppliers, license information, comments, or additional document fields.
- Source IP addresses and account, scan, or integration identifiers associated with Customer submissions.
- Personal Data in findings, triage notes, notification destinations, support requests, or requested diagnostic information.
- Credentials the Customer provides through the designated controls for registry scans or integrations, where they relate to a person.
- Workspace user data: email addresses, identity-provider account identifiers, roles, department membership, time of last sign-in and of acceptance of the terms, and audit-log entries (including email and network addresses) of the Customer's authorized users, to the extent made available to the Customer within the Service.
- Commit author and committer names and email addresses where included in commit metadata or SBOMs.
- Container image content retrieved for an authorized registry scan. TuxCare holds the image in temporary storage only to generate an inventory (SBOM) and deletes it when the scan completes. TuxCare keeps the inventory with the Workspace data and deletes it in accordance with paragraph (h).
- Email addresses of people invited to the Workspace by the Customer's administrators.

Package names, versions, graphs, hashes, image digests, and operating system data are technical data. They can become Personal Data when linked to individuals. The Portal can retain the whole submitted document, including fields it does not use for analysis. Ordinary dependency submission does not require source code, sensitive Personal Data, passwords, or private keys.

(d) Processing continues for the period needed to provide the Service under Customer's instructions. Return and deletion after that period follow clause 3.1(i) and paragraph (h).

(e) Sensitive Data Transferred: The Parties do not anticipate the transfer of sensitive data.

(f) Data subjects can include Customer's employees, contractors, administrators, and service provider contacts. They can also include authors, suppliers, and other people whose identifiers appear incidentally in Customer's submitted documents. Customer remains responsible for notices, lawful instructions, and authority to provide their data.

(g) Personal Data is stored and processed in the following regions and countries:

- hosting of servers and databases — Hetzner Online GmbH, Falkenstein, Germany (EU);
- backups and archives — Hetzner Online GmbH, Germany (EU), and Amazon Web Services, Inc., United States;
- DNS and delivery of Workspace email — Cloudflare, Inc., United States;
- business email and document storage used by TuxCare staff — Google LLC, United States.

The transfer mechanism for each provider is stated in Annex 3. TuxCare will notify the Customer of any change to the regions and countries listed in this paragraph in accordance with clauses 3.1(k) and 4.4.

(h) Duration and retention. TuxCare processes Customer Personal Data for the term of the Main Agreement and for the period necessary to return or delete it in accordance with clause 3.1(i). The Customer may delete the Workspace at any time through the controls provided in the Service; the Workspace stops at once, and its data is permanently removed from the active database thirty (30) days after the deletion. The Service keeps a limited number of scans per repository and deletes older scans automatically; finding history may remain after an older scan is deleted. A free Workspace without activity may be retired: TuxCare notifies the Customer after approximately twelve (12) months without activity, may suspend the Workspace after approximately thirteen (13) months and may delete it after approximately fifteen (15) months, and makes an archive export of the Workspace data available to the Customer before deletion. A restored backup remains subject to the Customer's deletion instruction. TuxCare applies clause 3.1(i) to all such copies. An archive does not create a right to retain Customer Personal Data for an unrelated purpose. Retention required by applicable law remains subject to restricted access and purpose limitation.

ANNEX 2 – TECHNICAL AND ORGANIZATIONAL MEASURES

This Annex describes the controls used for the applicable hosted service. It supplements clause 3.1(c) and the information for Annex II of the SCCs. A separate written security schedule controls any stronger commitments within its scope.

- The hosted service uses HTTPS for customer traffic and secure session cookies for browser access.
- Workspace identity and authorization limit access to the selected account. Supported roles, departments, and Token scopes restrict permitted actions and repositories.
- The hosted application uses database controls to restrict tenant access. Privileged service and operator access have separate authority.
- The service seals stored registry and identity provider secrets with authenticated encryption. This statement does not assert encryption of every database field.
- The service records account actions and operational access events to support security and investigation.
- Intake checks supported document formats, authentication, body size, and relevant Token scope before it stores a scan.
- TuxCare restricts personnel access and applies confidentiality duties under clause 3.1(d).
- TuxCare support staff use a read-only view of a Workspace to give support.
- Backup, recovery, data removal, and incident response follow the notified service arrangements and this DPA.

These measures do not assert that the SecureChain Portal holds a particular certification. They do not change the breach notice duty in clause 3.1(e) or the rights in the applicable SCCs.

ANNEX 3 – LIST OF SUB-PROCESSORS

TuxCare engages the following Sub-processors. The transfer mechanism relied on for each Sub-processor is stated in the table. Any Sub-processor added under clause 4.4 will be listed here together with its transfer mechanism.

Sub-processor	Location	Security certification	Purpose of processing	Transfer mechanism
Hetzner Online GmbH	Falkenstein, Germany	ISO 27001	Hosting of servers and databases Backups	Not required (EEA)
Amazon Web Services, Inc.	Northern Virginia and Ohio, United States	ISO 27001 SOC 2 Type 2	Backup and archive storage	Data Privacy Framework; SCCs as fallback (clause 6.5)
Cloudflare, Inc.	United States (global network)	ISO 27001 SOC 2 Type 2	DNS for the service domains Delivery of Workspace email (Cloudflare Email Service)	Data Privacy Framework; SCCs as fallback (clause 6.5)
Google LLC	United States	ISO 27001 SOC 2 Type 2	Business email and document storage (Google Workspace) used by TuxCare staff, for example, for support correspondence	Data Privacy Framework; SCCs as fallback (clause 6.5)