# SecureChain Portal Privacy Policy

Version 1.1
Effective date: November 09, 2026

## 1. INTRODUCTION

At TuxCare, Inc. (“TuxCare,” “We,” “Us,” or “Our”), we prioritize your privacy and protect your personal information. This SecureChain Portal Privacy Policy (this “Privacy Policy”) describes how we collect, use, share, and safeguard Personal Data in the SecureChain Portal, its APIs, and related CLI workflows. It covers the SecureChain Portal at https://sc.tuxcare.cloud, the Workspaces at their own subdomains (for example, name.sc.tuxcare.cloud), the TuxCare sign-in service at https://auth.tuxcare.cloud, the SecureChain CLI, and related account and support communications. It does not cover employees or candidates, or a third party’s own services.

TuxCare acts as Data Controller for account administration, access security, billing, and its own business communications. For Personal Data in inventories, SBOMs, and other Customer Data that we process under your instructions, TuxCare acts as Data Processor. We may act as sub-processor if you act for another controller. The SecureChain Portal Data Processing Addendum, published at https://tuxcare.com/legal/securechain-portal-data-processing-addendum/, governs that processing.

“Personal Data” or “Personal Information” means information that identifies, relates to, or can reasonably identify an individual, directly or indirectly. Technical data can contain Personal Data. An authenticated dependency report is not anonymous merely because it omits a repository name.

## 2. WHO WE ARE

TuxCare, Inc., registered at 20791 Three Oaks Pkwy, #980, Estero, FL 33929, USA, is a leading technology company dedicated to developing innovative software solutions that enhance server stability, security, and performance. Originally established as a specialized brand under Cloud Linux Software, Inc., TuxCare officially transitioned into a standalone entity, TuxCare, Inc., in 2026.

TuxCare provides an integrated ecosystem of security and stability solutions designed to maximize uptime and protect critical infrastructure. Our services encompass automated, real-time vulnerability management for kernels and system libraries, extended security maintenance for software stacks that have surpassed their official support lifecycles, and technical support for enterprise Linux environments to ensure long-term operational reliability.

## 3. WHAT INFORMATION WE COLLECT AND PROCESS

### 3.1 Information You Provide

When you interact with us via our websites or any sites or Services that link to this Privacy Policy or use the TuxCare products, we may collect Personal Data and other information from you, as further described in this Privacy Policy.

We ask that you do not share any sensitive personal information (such as authentication information) with us in general text fields, such as support tickets or forum posts. In cases where our support engineers require access to your systems for diagnostic purposes, they may request your access information. This request will always be made via a dedicated, secure form for safe transmission. Please use only the provided secure form and never share requested information directly in a support ticket, chat, or email. You are responsible for any data shared in violation of this instruction, and TuxCare shall have no liability for any sensitive data transmitted outside of our designated secure channel.

**3.1.1 Account and Sign-up Information.** We collect Personal Data when you register for a TuxCare account, modify user information, complete a purchase for our services, or provide any other related information to access or utilize our Services. This includes names, telephone

numbers, physical addresses, email addresses, and, if applicable, company names or tax ID numbers.

**3.1.2 Payment Information.** We collect billing and payment details. This includes your billing address and designated contact. Payment data (such as credit card or bank account numbers) is handled solely as authorized by you and processed by secure, PCI-DSS-compliant third-party providers using encrypted methods. TuxCare does not store full payment card details on its own servers.

**3.1.3 Communications Data.** Information relating to any communication with us, including the content of emails, tickets, forum postings, and testimonials, as well as recordings, transcripts, and AI-generated summaries of business meetings conducted via video conferencing tools.

**3.1.4 Support and Diagnostic Data.** Information provided for troubleshooting, including, without limitation, IP addresses, temporary credentials or access tokens strictly necessary to access systems for troubleshooting purposes, a list of running processes, and relevant configuration settings necessary for troubleshooting purposes.

### 3.2 Technical and Server Information

When you use SecureChain Services, and where applicable other TuxCare products, we collect data from the server environment:

- **Server Identifiers.** This may include information connected to authorized users, such as user identifiers and IP address information.

### 3.3 Device and Usage Data

We process source IP addresses, request times, access and security events, and technical client information. You sign in through the TuxCare sign-in service with a sign-in provider that you choose: Google, GitHub, or Microsoft. The provider handles your account data under its own privacy policy (the Google Privacy Policy, the GitHub General Privacy Statement, or the Microsoft Privacy Statement). We never see the password of your account at the provider.

Google. From Google, we receive your email address, whether Google has verified it, your Google account ID, and, for a Google Workspace account, the domain of your organization. Google also sends your name and profile picture; the sign-in service discards them and does not pass them on. We do not get access to your Gmail, Google Drive, contacts, calendar, or other Google data, and we do not keep the access token that Google issues.

GitHub. If you sign in with GitHub, you allow us to read your GitHub profile and the email addresses of your GitHub account (the GitHub scopes read:user and user:email). From GitHub, we receive your GitHub account ID, your username, your name, your profile picture, the public email address and the other fields of your profile, and the email addresses of your account, with whether each is your primary address and whether GitHub has verified it. The sign-in service uses your GitHub account ID, your primary email address, and whether GitHub has verified it; if GitHub names no primary address, it uses the public email address of your profile and treats it has not verified. It discards the other data and does not pass it on. We do not ask for access to your repositories, code, or organizations, and we do not keep the access token that GitHub issues.

Microsoft. You can sign in with a work or school account or with a personal Microsoft account. If you sign in with Microsoft, you allow us to read your basic profile and your email address (the Microsoft scopes openid, email, and profile). From Microsoft, we receive your email address (if your account has one), whether Microsoft has verified the owner of the domain of that address, your object ID and tenant ID, your name and username, and technical data of the sign-in. The sign-in service uses your object ID, your tenant ID, your email address, and whether the domain is verified; if Microsoft does not say that the

domain is verified, it treats the address as not verified. It discards the other data and does not pass it on. We do not ask for access to Microsoft Graph, your mail, files, contacts, or calendar, and we do not use or keep the access token that Microsoft issues. When you create a Workspace, we record its name, your account ID and email address as its owner, the time, and the network address of the request (for an IPv6 address, only the first half, the /64 network). When you sign in to the CLI in your browser, we record your email address, account ID, the network address of the CLI, and the device name and version it reports. Workspace records include user roles, department membership, Tokens and their scope, the time of each member's last sign-in and acceptance of the terms, and audit events with the email and network address of each person. Records of legal acceptance identify the person (email address and account ID), the legal name of the organization, the Workspace, the version of each document, the time and network address of the acceptance, and whether it came from the signup, the web app or the CLI sign-in. We keep them for legal and audit purposes and to establish, exercise or defend legal claims.

### 3.4 AI Chatbot Interaction

When you interact with our AI-powered chatbot, we process the content of your queries and the generated replies to facilitate your request. While conversation history is stored to enhance service quality, this data is not fingerprinted or directly linked to your individual identity. All processing occurs on secure servers located within the European Union. Notably, neither TuxCare, Inc. nor our AI provider utilizes your conversation data to train artificial intelligence models. To protect your privacy, we advise against including sensitive personal data within the chatbot conversation. This section applies only where TuxCare makes an AI chatbot available in the SecureChain Portal or on a TuxCare website you use. Where no such chatbot is offered, no processing under this section takes place.

### 3.5 Cookies and Tracking Technologies

The SecureChain Portal, the Workspaces and the TuxCare sign-in service use only strictly necessary cookies. They keep you signed in and protect the sign-in against forgery. The pages also keep two values in your browser's local storage: whether you closed the cookie banner, and the light or dark theme you selected. We use no analytics, advertising, or tracking cookies, and the pages load no content from other companies. The cookie notice lists each cookie with its purpose and duration. Your identity provider applies its own cookie notice when you sign in there. If TuxCare introduces optional analytics or marketing cookies, we will provide the required notice and consent controls before use.

### 3.6 SecureChain Dependency Reports and SBOMs

A dependency report can contain package names, namespaces, versions, package URLs, direct or transitive relationships, coverage information, and aggregate counts. It can also contain the client version and platform, timestamps, content hashes, a project label, and repository identity that the client includes. Repository identity can include a remote URL, a branch or tag, and a commit identifier.

An SBOM can contain dependency graphs, artifact hashes, license information, relative file paths, and component metadata. Image inventories can include the registry path, image tag and digest, operating system, platform, and package qualifiers. The Portal retains the submitted document as well as the fields it extracts. A third-party SBOM can therefore expose extra fields, comments, or identifiers that matching does not use.

Private package names are not automatically hidden or hashed. Their names and versions can identify internal projects or people. The Services analyze dependency metadata and do not require source code for ordinary dependency submission. Do not include source code, passwords, private keys, unrelated Personal Data, or sensitive data in reports, SBOMs, or general support fields.

The CLI sends the name and version of each package, the repository URL, branch and commit, and the path of the project in the repository. It never sends source code or file contents, environment variables or secrets, or a username or password contained in the repository URL. The command securechain sbom --

preview shows the exact upload and sends nothing. An authorized CI workflow can submit on later runs without another prompt.

Use your own Workspace endpoint and Token for private projects.

### 3.7 Findings, Integrations and Credentials

We store findings, severity and exploitation information, scan comparisons, triage decisions, notes, and notification preferences. Your authorized users can see data within their account and role scope. We send findings and related metadata to email, Slack, and webhook destinations your administrators configure. Workspace email, such as invitations and alerts, is sent through Cloudflare Email Service.

If you enable registry scans, we process the registry credentials, selected image references, and image content needed to generate an inventory. The scan service can retrieve the selected image. The scan service holds the image in temporary storage only while it generates the inventory, and deletes the image when the scan completes. We keep only the inventory with the Workspace data. We process identity provider settings and integration secrets only through the controls for those functions.

### 3.8 Local and Self-Hosted Use

TuxCare receives a report only when a client or integration sends it to a TuxCare endpoint. A local preview does not submit its preview bytes. Other network actions depend on the command and version. If you run a self-hosted Portal, your organization controls its stored Customer Data. TuxCare can still receive data through package access, licensing, support, or an integration you configure.

## 4. HOW WE USE YOUR INFORMATION

Any of the information we collect from you may be used for the following purposes and related lawful bases:

| Purpose of processing | Lawful basis | Types of Personal Data |
|---|---|---|
| To provide our products and services to you, including: setting up and maintaining accounts, communicating with you, and informing you about product updates, improvements, and essential technical changes. | Contract<br>Legitimate Interest | Account and Sign-up Information<br>Payment Information<br>Communications Data<br>Technical and Server Information |
| To process financial transactions, generate invoices, manage payments, track billing history, and ensure accurate financial record-keeping related to our products and services | Contract<br>Legal Obligation | Account and Sign-up Information<br>Payment Information<br>Communications Data |
| To provide support services, including responding to client support requests, assisting with product usage, diagnosing and resolving technical issues, and providing guidance related to the operation of the services.<br>Where explicitly requested and authorized by the client, this may include temporary and limited remote access to the client's server solely for the purpose of investigating and resolving specific technical issues. | Contract<br>Legitimate Interest<br>Consent | Account and Sign-up Information<br>Communications Data<br>Support and Diagnostic Data<br>Technical and Server Information<br>AI Chatbot Interaction |
| Sending promotional materials, newsletters, and invitations to webinars, including information about products, services, and updates, where permitted by applicable law, with the ability to opt out at any time. | Consent<br>Legitimate Interest | Account and Sign-up Information<br>Communications Data<br>Device and Usage Data |

| Purpose of processing | Lawful basis | Types of Personal Data |
|---|---|---|
| To record and process meeting recordings and transcripts from sales and business calls, and generate AI-assisted summaries of meeting content to manage and maintain our business relationships. | Legitimate Interest<br>Consent | Account and Sign-up Information<br>Communications Data |
| For our own business purposes, including conducting customer surveys, performing data analysis, collecting and assessing feedback, identifying usage trends, providing training and customer service, and similar business functions.<br>This information supports internal reporting.<br>It allows us to generate email lists for sending maintenance updates and contact clients for feedback or product usage inquiries. | Legitimate Interest | Account and Sign-up Information<br>Communications Data<br>Device and Usage Data<br>Technical and Server Information |
| We process your personal data to comply with legal obligations and safeguard the security and integrity of our systems and services. This includes fulfilling legal requirements, protecting the rights and safety of individuals and property, and investigating potential violations of our policies.<br>We also use your account and log file information to analyze how our services are used, monitor access patterns, and enhance your navigation experience.<br>For regulatory, security, and debugging purposes, we collect and log IP addresses, associate them with other personal data you provide (e.g., name, email address, and physical address), and use this data to detect, prevent, and respond to security incidents or malicious activities. | Legitimate Interest<br>Legal Obligation | Account and Sign-up Information<br>Communications Data<br>Device and Usage Data<br>Technical and Server Information |
| To store inventories, match advisories, evaluate stored scans again, compare scans, provide recommendations, and send configured alerts. We do not need another upload to evaluate an inventory we retain. | Customer instructions and the DPA for Customer Personal Data; contract or legitimate interests for our own account and security processing, as applicable. | Dependency reports, SBOMs, repository and image metadata, findings, and configured recipient details. |
| To administer Workspaces, protect access, apply limits, and record legal acceptance when those controls apply. | Contract; legitimate interests; legal obligation where applicable. | Identity and account records, access logs, Tokens and their scope, and acceptance records. |

## 5. HOW WE SHARE PERSONAL DATA

### 5.1 Service Providers

The table below retains TuxCare's general list of service providers. It does not mean every provider receives every SecureChain submission. The Sub-processors that process Customer Personal Data under the DPA, and their locations, are those listed in Annex 3 to the DPA; a provider that appears in the table below but not in Annex 3 does not process Customer Personal Data submitted to the SecureChain Portal.

For the SecureChain Portal, Hetzner Online GmbH hosts the servers, databases and backups in Falkenstein, Germany; Amazon Web Services, Inc. also stores backups in the United States; and Cloudflare, Inc. provides DNS and sends Workspace email. We do not send your private inventories to a marketing provider merely because you use Portal.

| Service Provider | Processing location | Purpose | Categories of data shared |
|---|---|---|---|
| Amazon Web Services, Inc. | United States (primary)<br>EU regions for certain services | Hosting & infrastructure | Account and Sign-up Information<br>Support and Diagnostic Data<br>Technical and Server Information |
| Atman Sp. z o.o. | Poland, EU | Hosting & infrastructure | Account and Sign-up Information<br>Support and Diagnostic Data<br>Technical and Server Information |
| Hetzner Online GmbH | Germany & Finland (EU)<br>United States | Hosting & infrastructure | Account and Sign-up Information<br>Support and Diagnostic Data<br>Technical and Server Information |
| Hivelocity, Inc. | United States | Hosting & infrastructure | Account and Sign-up Information<br>Support and Diagnostic Data<br>Technical and Server Information |
| Cloudflare, Inc. | United States / global edge network | Content delivery, DNS, network security & email delivery | Account and Sign-up Information<br>Communications Data<br>Technical and Server Information |
| Acronis International GmbH | Germany | Data backup | All categories of Personal Data contained in backed-up systems |
| HubSpot, Inc. | United States | CRM, marketing & sales support | Account and Sign-up Information<br>Communications Data |
| Chili Piper, Inc. | United States | Meeting scheduling | Account and Sign-up Information<br>Meeting scheduling data |
| Zendesk, Inc. | United States (and other regions) | Customer support ticketing | Account and Sign-up Information<br>Communications Data<br>Support and Diagnostic Data |
| Google LLC | United States and other countries (global) | Email, documents, video calls | Communications Data<br>Account and Sign-up Information<br>Other Personal Data contained in messages, files, and meetings |
| Zoom Communications, Inc. | United States / global | Video meetings & webinars | Account and Sign-up Information (name, email)<br>Communications Data |
| ChargeBee, Inc. | United States | Subscription billing & invoicing | Account and Sign-up Information<br>Payment Information |
| Stripe LLC | United States (and global) | Payment processing | Account and Sign-up Information<br>Payment Information |
| Dilisense GmbH | Switzerland<br>Germany (EU) | KYC / sanctions & PEP screening | Account and Sign-up Information |
| Snowflake, Inc. | United States | Analytics & reporting | Account and Sign-up Information<br>Technical and Server Information (aggregated for analytics) |
| Google LLC (Looker) | United States | Analytics & reporting | Account and Sign-up Information<br>Technical and Server Information (aggregated for analytics) |

### 5.2 Affiliates

We may share Personal Data with our current and future affiliates and group companies, including Cloud Linux Software, Inc., 20791 Three Oaks Pkwy, #980, Estero, Florida 33929, United States, for purposes consistent with this Privacy Policy, such as shared business infrastructure, administration, customer support, and service delivery. Any such sharing is subject to intra-group data protection arrangements ensuring an equivalent level of protection.

### 5.3 Marketing Communications

We share limited Personal Data with the marketing and sales communication providers listed in Section 5.1 only where you have opted in to receive marketing communications, and solely to deliver relevant content, updates, and promotions. You may opt out of marketing communications at any time by following the unsubscribe instructions in any marketing message or by contacting us directly. We will promptly honor your request.

### 5.4 Third-Party Widgets

Our blogs and forums might contain widgets and social media features, such as the X “Post” or Facebook “like” buttons. These widgets and features may collect your IP address and which page you are visiting on the sites, and may set a cookie to enable the feature to function properly. Widgets and social media features are hosted either by the first party or a third party. Your interactions with these features are governed by the privacy policy of the company providing them.

### 5.5 Legal and Regulatory Disclosure

We may share your information as required by law, such as to comply with statutory requirements, court orders, or other legal processes. We may also disclose information when we believe in good faith that it is necessary to protect our rights, your safety, or the safety of others, investigate suspected fraud or security issues, or respond to lawful government requests.

### 5.6 Corporate Transactions

If TuxCare undergoes a merger, acquisition, or sale of all or part of its assets, your personal information may be transferred as part of that transaction. In such cases, we will notify you via email and/or by posting a prominent notice on our website, informing you of any changes in ownership, the potential new uses of your personal information, and the choices available to you regarding your data.

### 5.7 Workspace Members and TuxCare Support Staff

People with the member or admin role in a Workspace can see the email addresses of its other users, and Workspace admins can also see its audit log. TuxCare support staff can open a read-only view of a Workspace to give support.

## 6. HOW WE TRANSFER PERSONAL DATA INTERNATIONALLY

### 6.1 International Transfers and Safeguards

This Privacy Policy applies regardless of where Personal Data is processed. The servers and databases of the SecureChain Portal are in a data center in Germany; TuxCare, Inc. and some of its service providers are in the United States. We have implemented rigorous safeguards to ensure your data remains protected. For transfers from the European Economic Area (“EEA”), Switzerland, or the United Kingdom (“UK”), we rely first on our certification under the EU-U.S. Data Privacy Framework, its UK Extension and the Swiss-U.S. Data Privacy Framework. Where that certification does not cover a transfer, or ceases to be a valid transfer mechanism, the Standard Contractual Clauses and the UK International Data Transfer Addendum apply automatically, supplemented by technical measures such as industry-standard encryption and TLS for hosted sites.

### 6.2 Data Privacy Framework Notice

Where TuxCare relies on an active certification under the EU-U.S. Data Privacy Framework, its UK Extension, or the Swiss-U.S. Framework, the applicable Principles govern that transfer. TuxCare uses another valid safeguard where that certification does not cover a transfer. The notices below apply to Personal Data TuxCare receives in reliance on an applicable Framework.

If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles and/or the UK DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) Program and to view our certification, please visit https://www.dataprivacyframework.gov/.

Concerning personal data received or transferred under the Data Privacy Frameworks, TuxCare, Inc. is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission (FTC). The Federal Trade Commission has jurisdiction over TuxCare's compliance with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF).

***Individual Rights and Accountability***

Under the Data Privacy Framework, individuals in the European Union, the United Kingdom, and Switzerland have the right to obtain confirmation of whether we maintain personal information relating to them in the United States and may request access to, correction of, or the deletion of inaccurate data by directing their query to privacy@tuxcare.com.

We provide an opt-out or opt-in choice before we share your data with third parties other than our agents, or before we use it for a purpose other than that for which it was originally collected. TuxCare remains responsible and liable under the DPF Principles if third-party agents that it engages to process personal data on its behalf do so in a manner inconsistent with the DPF Principles, unless we prove we are not responsible for the event giving rise to any damage. Additionally, we may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

***Dispute Resolution***

If a privacy complaint or dispute relating to Personal Data received by TuxCare, Inc. in reliance on the Data Privacy Framework (or any of its predecessors) cannot be resolved through our internal processes, we have agreed to participate in the VeraSafe Data Privacy Framework Dispute Resolution Procedure. Subject to the terms of the VeraSafe Data Privacy Framework Dispute Resolution Procedure, VeraSafe will provide appropriate recourse free of charge to you. To file a complaint with VeraSafe and participate in the VeraSafe Data Privacy Framework Dispute Resolution Procedure, please submit the required information here: https://www.verasafe.com/privacy-services/dispute-resolution/submit-dispute/.

***Binding Arbitration***

If your dispute or complaint related to your Personal Data that we received in reliance on the Data Privacy Framework cannot be resolved by us, nor through the dispute resolution mechanism mentioned above, you may have the right to require that we enter into binding arbitration with you under the Data Privacy Framework "Recourse, Enforcement and Liability" Principle and Annex I of the Data Privacy Framework.

## 7. HOW WE STORE AND SECURE PERSONAL DATA

### 7.1 Data Storage and Security

We implement a variety of security measures to maintain the safety of your personal information when you place an order or enter, submit, or access your personal information. We offer the use of a secure server. All supplied information is transmitted via Transport Layer Security (TLS) technology and then stored in our database to be accessed only by those authorized with special access rights to our systems, and are required to keep the information confidential. Credit card information is transmitted directly to the payment processor and is not stored on our servers. If you have any questions about the security of your personal information, you can contact us at privacy@tuxcare.com or visit our Security and Compliance web section.

### 7.2 Retention of Personal Data

We retain inventories and findings while they are needed to provide the Workspace service. The Service keeps a limited number of scans per repository and deletes older scans automatically; finding history can remain after an older scan is deleted. Stored inventories can be evaluated against later advisories for as long as we retain them. The table below shows how long we keep SecureChain data; Annex 1(h) of the DPA sets out the same rules for Customer Personal Data.

| Data | How long we keep it |
|---|---|
| Data your identity provider sends during sign-in | 10 minutes for a sign-in; 1 hour for an access token |
| Sign-in sessions (cookies) | 30 minutes on sc.tuxcare.cloud; 12 hours in a Workspace |
| CLI sign-in records | One day after the sign-in request expires |
| Workspace data: user records, audit log, scans, findings, and inventories generated by registry scans | While the Workspace exists. When the Workspace is deleted, it stops at once, and its data is removed 30 days later. |
| Inactive free Workspaces | Notice after about 12 months without activity, suspension after about 13 months, deletion after about 15 months. An archive export is available before deletion. |
| Workspace directory record (name, owner and creation record) | Kept after the Workspace is deleted, so that no new Workspace can take the same name |
| Records of legal acceptance | As long as the Workspace exists, also after the person is removed from it. 7 years after the Workspace is deleted. |

Deleting a Workspace does not immediately erase backups. Backup copies are overwritten in their normal cycle and remain subject to the DPA until then. Contact privacy@tuxcare.com for a deletion request.

Revoking a Token, stopping uploads, or removing a local client does not delete data already held by the Portal. Access logs, security records, and legal acceptance records can have separate retention periods based on their purpose. We do not retain Customer Personal Data for unrelated use after its authorized purpose ends.

How long we keep the information we collect about you depends on the type of information and how we collect and store it. We retain financial and transactional information, including billing records and payment history, for a period of seven (7) years to comply with our legal, tax, and accounting obligations.

We retain Personal Data only where we have an ongoing legitimate business need to do so, such as resolving disputes or enforcing our agreements. Information associated with our operational history may be retained for business purposes in an anonymized form once the primary retention period has expired.

When we no longer have a legitimate business need to process your Personal Data, we securely delete or anonymize it. For example, support ticket histories are anonymized by removing all personal identifiers, allowing us to retain the technical data for service improvement and statistical purposes. We will also delete this information at an earlier date if you so request, as described in Section 8 (Your Privacy Rights).

## 8. YOUR PRIVACY RIGHTS

Just as we have our rights and obligations to process your personal information, you also have certain rights to process your personal data. These rights include:

- **Right of access.** In accordance with Art. 15 GDPR, you may have the right to obtain confirmation from us as to whether or not your personal data is processed by us, and, where that is the case, to request access to your personal data. The information about personal data processing includes the purposes of the processing, the categories of personal data concerned, and the recipients or categories of recipients to whom your personal data have been or may be disclosed. However,

this is not an absolute right, and the interests of other individuals may restrict your right of access. Also, you may have the right to obtain a copy of your personal data that is undergoing processing. For additional copies requested, we may charge a reasonable fee based on administrative costs.

- **Right to rectification.** In accordance with Art. 16 GDPR, you may have the right to obtain from us the rectification of inaccurate personal data. Depending on the purposes of the processing, you may have the right to have incomplete personal data completed, including by means of providing a supplementary statement.
- **Right to erasure (right to be forgotten).** In accordance with Art. 17 GDPR, you have the right to request that we delete your personal data. Please keep in mind that we may keep your personal data if it is still necessary for:
  a. fulfilling our legal obligation;
  b. archival, historical, or scientific research or statistical purposes; or
  c. determination, exercise, or defense of our legal claims.
- **Right to restriction of processing.** In accordance with Art. 18 GDPR, you have the right to request that we restrict the processing of your personal data. In this case, the respective personal data will be marked accordingly and may only be processed by us for certain purposes.
- **Right to personal data portability.** In accordance with Art. 20 GDPR, you have the right to receive the personal data concerning you, which you have provided to us, in a structured, commonly used, and machine-readable format and/or to request the transfer of this personal data to another entity.
- **Right to withdraw consent.** In accordance with Art. 7(3) GDPR, where processing is based on your consent, you have the right to withdraw that consent at any time. Withdrawal does not affect the lawfulness of any processing carried out prior to withdrawal. To withdraw your consent, please contact us at privacy@tuxcare.com.
- **Right to object.** In accordance with Art. 21 GDPR, you have the right to object at any time to the processing of your personal data where that processing is based on our legitimate interests or carried out in the public interest. Where you object, we will cease processing your personal data unless we can demonstrate compelling legitimate grounds for the processing that override your interests, rights, and freedoms, or where processing is necessary for the establishment, exercise, or defense of legal claims. You also have the right to object at any time to the processing of your personal data for direct marketing purposes, including profiling to the extent it relates to such direct marketing.
- **Right to lodge a complaint.** In accordance with Art. 77 GDPR, you have the right to lodge a complaint with a supervisory authority, in particular in the EU Member State of your habitual residence, place of work or place of the alleged infringement. In the United Kingdom, you may complain to the Information Commissioner's Office (ICO), and in Switzerland to the Federal Data Protection and Information Commissioner (FDPIC). We encourage you to contact us first at privacy@tuxcare.com so that we can try to resolve your concern.

Please note that to protect Personal Information, we may verify your identity by a method appropriate to the type of request you are making.

We will respond to your request to change, correct, or delete your data within a reasonable time frame and notify you of the action we have taken. In some instances, your rights may be limited, such as where fulfilling your request would impair the rights of others, our ability to provide a service you have requested, or our ability to comply with our legal obligations and enforce our legal rights.

## 9. CHILDREN'S ONLINE PRIVACY

TuxCare is committed to protecting the privacy of children. Our services are not intended for individuals under the age of 16, and we do not knowingly collect personal information from children under this age. If we learn that we have collected personal data from a child under 16 without parental consent, we will promptly delete that information.

Parents or guardians who believe their child has provided us with personal information can contact us as described below in Section 13 (How to Contact Us). We will take appropriate steps to provide access to, correct, or delete the child's data upon verification of your identity.

## 10. SUPPLEMENTAL ADDENDUM FOR CALIFORNIA RESIDENTS

### 10.1 Applicability

This section applies only to California residents. It describes how we collect, use, and share California consumers' Personal Information in our role as a business, and the rights applicable to such residents. If you are unable to access this Privacy Policy due to a disability or any physical or mental impairment, please contact us, and we will assist in supplying you with the information you need in an alternative format that you can access. For purposes of this section, "Personal Information" has the meaning given in the California Consumer Privacy Act ("CCPA"), as amended by the California Privacy Rights Act ("CPRA").

### 10.2 How We Collect, Use, and Share Your Personal Information

We might collect the following statutory categories of Personal Information:

- Identifiers, such as names, addresses, telephone numbers, and email addresses.
- Internet or network information, such as browsing and search history. We collect this information directly from your device.
- Geolocation data, such as an IP address. We collect this information from your device.
- Other personal information, in instances when you interact with us online, by phone, or by mail in the context of receiving help through our help desks or other support channels; participation in customer surveys or contests; or in providing the service.

The business and commercial purposes for which we collect this information are described in this Privacy Policy. The categories of third parties to whom we "disclose" this information for business purposes are described in this Privacy Policy.

### 10.3 Sensitive Personal Information

We do not ask you to include sensitive Personal Information in ordinary inventory submissions. Where a credential constitutes sensitive Personal Information, we process it through designated authentication or integration controls. We limit that processing to the service you request, access security, and purposes permitted by applicable law. We do not use it to infer personal characteristics or for unrelated advertising.

### 10.4 Your California Rights

You have certain rights regarding the Personal Information we collect or maintain about you. Please note these rights are not absolute, and there may be cases when we decline your request as permitted by law. Your rights include:

- **The right of access.** You may request that we disclose what Personal Information we have collected, used, and disclosed about you in the past 12 months.
- **The right to deletion.** You have the right to request that we delete Personal Information collected or maintained by us, subject to certain exceptions.

- **The right to correction.** You may request that we correct inaccurate Personal Information we hold about you.
- **The right to opt out of sharing or selling.** While TuxCare does not sell Personal Information to third parties, the CPRA also provides the right to opt out of certain “sharing” of Personal Information for targeted advertising purposes.
- **The right to non-discrimination.** You will not receive any discriminatory treatment when you exercise one of your privacy rights.

TuxCare does not sell Personal Information to third parties (under California Civil Code §§ 1798.100–1798.199, also known as the California Consumer Privacy Act of 2018).

## 11. USE OF AUTOMATED DECISION-MAKING TOOLS AND AI-ASSISTED TECHNOLOGIES

SecureChain automatically compares dependency metadata with advisory and catalogue data. Your selected CI rules can cause a build to pass or fail based on those results. You control those rules and remain responsible for your deployment decisions. This function evaluates software components. It does not make decisions about an individual’s eligibility, employment, or access to credit. TuxCare does not use nonpublic SecureChain Customer Data to train a general-purpose AI model unless you separately authorize that use.

We use artificial intelligence (AI) and machine learning technologies, including tools provided by third-party AI providers, to support our services and business operations, such as responding to customer inquiries, assisting our support engineers in analyzing and resolving technical issues, summarizing business communications, and improving our internal productivity and service quality. Wherever AI technologies process Personal Data, the following principles apply:

- Third-party AI providers act as our data processors under data processing agreements and are not permitted to use your Personal Data to train or improve their AI models;
- AI tools support human decision-making and do not make solely automated decisions that produce legal or similarly significant effects on you;
- AI-generated outputs used in our interactions with you are subject to human review before any further use;
- We apply data minimization and technical safeguards to limit the Personal Data submitted to AI tools.

We advise against including sensitive personal data in any AI-assisted interaction. Current examples of how we use AI technologies include:

- **Customer support chatbot.** Where offered (see Section 3.4), our AI-powered chatbot processes the content of your queries and their replies to deliver informational responses in real time. Its function is strictly consultative.
- **Support assistance tools.** Our support engineers may use AI-assisted tools to help analyze support requests and diagnostic information and draft responses, subject to the data minimization and human review principles above.
- **Meeting summarization.** We use AI-assisted tools to generate summaries of recorded sales and business meetings for internal record-keeping and relationship management; summaries may be associated with your company record in our CRM system. Before any recorded meeting, participants are notified that the session may be recorded, transcribed, and summarized using AI tools, and may decline at any time before or during the meeting; where a participant declines, the recording will not proceed or will be stopped immediately.

## 12. CHANGES TO THIS PRIVACY POLICY

TuxCare may update this Privacy Policy from time to time to reflect changes in our practices or for legal and regulatory reasons. We will notify you of any updates by posting the revised policy on this page and updating the effective date at the top. Changes become effective immediately upon posting. We encourage you to review this Privacy Policy periodically to stay informed about how we protect your information.

## 13. HOW TO CONTACT US

If you have any questions about this Privacy Policy, would like more information about how we manage your personal data, or need to contact our Data Protection Officer (DPO), please reach out to us at:

TuxCare, Inc. — Email: privacy@tuxcare.com

### *Our Representative in the European Union (EU)*

In accordance with Article 27 of the General Data Protection Regulation (GDPR), we have appointed a representative in the EU to act as a point of contact for data subjects and supervisory authorities. You can contact our EU representative at:

IT.LAW GmbH

- TuxCare, Inc. – Colmantstraße 15, 53115 Bonn, Germany
- Email: art-27-rep-tuxcare@it.law

### *Our Representative in the United Kingdom (UK)*

In accordance with Article 27 of the UK General Data Protection Regulation (UK-GDPR), we have appointed a representative in the UK to act as a point of contact for data subjects and supervisory authorities. You can contact our UK representative at:

Rickert Services Ltd UK

- TuxCare, Inc. – PO Box 1487, Peterborough PE1 9XX, United Kingdom
- Email: art-27-rep-tuxcare@rickert-services.uk