CLIENTS PRIVACY POLICY

Effective: 29 January 2025

Version 1.1

1. **INTRODUCTION**

Welcome to CloudLinux.
At Cloud Linux Software, Inc., Doing Business As TuxCare (hereinafter - “CloudLinux,” “We,” “Us,” or “Our”), we prioritize your privacy and are dedicated to protecting your personal information. This Privacy Policy outlines how we collect, use, share, and safeguard client personal data in compliance with relevant data protection laws, such as the General Data Protection Regulation (GDPR).

Our goal is to provide clear information about the types of personal data we collect, why we process it, and your rights as a CloudLinux client. This Privacy Policy applies to all personal information gathered directly or through our online platforms in relation to all products and services under CloudLinux, Imunify, and TuxCare brands (“Service” or collectively “Services”).

CloudLinux may update this Privacy Policy at any time, at our sole discretion. Any changes will become effective immediately upon posting. For significant updates, we will make reasonable efforts to notify you via a website banner, email, or other methods. Your continued use of our Services after any update constitutes acceptance of the revised Privacy Policy. Should you find any terms unacceptable, you are advised to discontinue use of our Services.

As used in this Policy, “Personal Data” or “Personal Information” refers to any information that relates to, identifies, or can reasonably be used to identify an individual, directly or indirectly. This Policy applies to our customers and end-users and does not cover our current and former employees, candidates, or website users.

Data Processing Roles:

- **Data Controller:** When you sign up for our products and Services, CloudLinux acts as the controller of your personal data. We process this data to deliver our services, communicate relevant content, and enhance and promote our offerings.
- **Data Processor**: When our customers use our products and Services for their sales, marketing, or other business operations, CloudLinux acts as a processor (or service provider) of personal data on behalf of these customers, who are the data controllers, in line with the CloudLinux Data Processing Agreement.

2. **WHO WE ARE**

Cloud Linux Software, Inc. is registered at 20791 Three Oaks Pkwy, #980, Estero, FL 33929, USA, is a technology company dedicated to developing and delivering innovative software solutions that enhance server stability, security, and performance across various environments. With a focus on empowering service providers, data centers, and web hosting companies, we design products to deliver increased reliability and security, tailored to meet the unique needs of our clients.

We operate under the following primary brands:

- **CloudLinux**: The foundational brand under which we offer products such as CloudLinux OS, a leading operating system for hosting providers that improve stability, density, and security in multi-tenant server environments.
- **Imunify:** Imunify is a leading brand in web security, offering a comprehensive suite of security solutions tailored for hosting providers to protect Linux-based web servers. The Imunify suite includes features like malware scanning, proactive defense, and advanced firewall protection, specifically designed to safeguard websites against evolving threats.
- **TuxCare**: Under the TuxCare brand, we deliver a suite of advanced security and support products, including KernelCare Enterprise, which provides automated live patching of Linux kernels; Endless Lifecycle Support (ELS), enabling extended security for end-of-life Linux systems, software languages, and software development frameworks; and Enterprise Support for AlmaLinux, which helps ensure optimal performance, security, and reliability of AlmaLinux systems. TuxCare is known for offering solutions that enhance the security and longevity of enterprise Linux systems.

As a global remote company, CloudLinux serves a diverse, worldwide client base, from hosting providers to enterprises, all while maintaining a strong commitment to data privacy and security in all of our operations. Whether acting as a data controller or processor, we adhere to stringent data protection practices and implement cutting-edge technologies to secure and manage data responsibly.

Our mission is not only to equip our clients with powerful, scalable tools but also to foster trusted relationships by respecting and protecting their personal information. Through this Privacy Policy, we aim to clearly communicate our privacy practices, provide transparency, and uphold the rights of individuals regarding their personal data.

3. WHAT INFORMATION WE COLLECT AND PROCESS

3.1. Information you provide to CloudLinux

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

3.1.1. Account and Sign-up Information

We collect Personal Data when you sign up for a CloudLinux/TuxCare account, create or modify user information, set preferences, or provide any other related information to access or utilize our Services. This Personal Data including names, addresses, telephone numbers, fax numbers, physical addresses, email addresses, credit card numbers, and, if applicable, company names, addresses, telephone numbers, fax numbers, physical addresses, email addresses, credit card numbers, or tax ID numbers as well as similar information concerning technical contacts, marketing contacts, and executive contacts within your company or organization.

3.1.2. Payment Information

We collect billing and payment information when you register for any paid products or services with CloudLinux. This may include details like your billing address and designated billing contact for your account. If you choose to provide payment information, such as a credit card or bank account number, we handle it in accordance with this Privacy Policy and solely as authorized by you.

To process payments, we use secure, PCI-DSS-compliant third-party payment providers who manage payment transactions through encrypted and secure methods. Your payment information is collected and processed directly by these providers, ensuring the highest standards of data security and protection.

3.2. Information we process on behalf of customers when they use our Services

3.2.1 CloudLinux OS

Only if you use CloudLinux OS Shared PRO and/or CloudLinux OS Solo, CloudLinux OS may indirectly collect information about visitors of any site hosted on a server that is using CloudLinux OS Shared PRO or CloudLinux OS Solo. One of the features of both Services (the feature`s name is X-Ray) tracks the time of the SQL request execution. To track the time and analyze the SQL request execution, the feature processes in an encrypted manner and stores the SQL requests in a depersonalized format. The SQL requests can consist of Personally Identifiable Information of the visitors of any hosted site. For more details please read and sign our CloudLinux OS Data Processing Agreement in the relevant License Agreement.

3.2.2. Imunify360

Only if you use Imunify360, Imunify360 collects information about visitors of any site hosted on a server protected by Imunify360. That information includes visitors' IP addresses, URI, browser information, screen resolution as well as other location & browser metadata. We might also collect HTTP/HTTPs query parameters, encrypted using one-way encryption (irreversible encryption used for comparison & analysis). If an attack is detected, we will collect HTTP parameters without using one-way encryption. We will still encrypt it to transfer it to our servers. For more details please read and sign our Imunify360 Data Processing Agreement in the relevant License Agreement.

3.2.3. ImunifyEmail

Only if you use Imunify Email, Imunify Email collects information about mail senders and recipients of any MTA agent protected by Imunify Email. That information includes sender/recipient mail addresses, IP addresses, message content, and SMTP headers. Arbitrary email message content may be used to enhance machine learning input data. The data is never stored outside customer premises but can be temporarily accessed by CloudLinux antispam engineers. It is never stored or transmitted in non-encrypted form and can be unencrypted to be loaded in RAM for processing purposes. For more details please read and sign our Imunify360 Data Processing Agreement in the relevant License Agreement.

3.2.4. Tuxcare

Only if you use Tuxcare products, specifically KernelCare, and/or ELS (Endless Lifecycle Support), and/or Enterprise Support for AlmaLinux, Tuxcare does not collect Personally Identifiable Information about end users on behalf of customers.

3.2.5. Server Information

If you use one of our products such as CloudLinux OS, KernelCare, Imunify360, or TuxCare™ products and services, we may collect certain non-Personally Identifiable Information concerning such software, its use, and the server upon which the software operates. This information includes (a) the licensed or unlicensed status of the software; (b) the source from which the license for the software was obtained (CloudLinux or CloudLinux reseller or partner); or (c) information about the server upon which the software is installed including (i) the public IP address, (ii) the operating system and (iii) the use of any virtualization technologies on such server ((a) through (c) collectively, "Server Information"), server uptime and server hardware information including CPU, memory, disks, motherboard. Additionally, "Server Information" may also include (x) information collected by CloudLinux from time to time concerning which features of the software are most often used to improve and make adjustments to the software; and (y) information collected from you by CloudLinux if you request technical support services including without limitation, IP addresses, usernames and passwords necessary to login to SSH, list of running processes and content of configuration files.

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.	Contract Legitimate Interest	Contact and account information Payment and purchase-related information Video, audio, and communication information Device and System Information
To process financial transactions, generate invoices, manage payments, track billing history, and ensure accurate financial record-keeping related to our	Contract Legitimate Interest Legal Obligation	Contact and account information Payment and purchase-related information

Products and Services		
To provide comprehensive technical assistance, troubleshoot product issues, and optimize user experience. This includes: responding to support requests, offering guidance on product usage, diagnosing and resolving technical problems, providing remote assistance at the client's explicit request, temporarily accessing client systems for targeted issue resolution, advising on suitable solutions based on the client's system analysis, and improving product functionality through insights gained from support interactions.	Contract Legitimate Interest Consent	Contact and account information Video, audio, and communication information Domain Names Login Credentials
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. We also may analyze data to identify clients with specific hosting panels installed or a particular number of users. This information supports internal reporting for tools such as CLOS, Imunify, and KernelCare. It allows us to generate email lists for	Legitimate Interest Legal Obligation	Contact and Account Information Usage Information Communication information

sending maintenance updates, and contact clients for feedback or product usage inquiries.		
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. We also use your account and log file information to analyze how our services are used, monitor access patterns, and enhance your navigation experience. 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 Legal Obligation	Contact and Account Information Usage Information Device and System Information

5. HOW WE SHARE PERSONAL DATA

5.1. Service Providers

We may share Personal Data with our third-party service providers to support our websites, products, and services. For example, we use service providers for data hosting, sales support, and customer support (Zendesk as a ticketing system, Zoom and Obsproject as the video calls providers) carrying out the Know Your Client process or processing your payment (Chargebee, Stripe, PayPal as a payment gateway). We may need to share your information with service

providers to provide information about products or services to you. We also work with service providers that assist us in building data analytics and reporting capabilities (Snowflake, Looker). These providers help us aggregate, analyze, and interpret data to better understand user behavior, improve operational efficiencies, and enhance our decision-making processes. In the context of customer support, we may also share necessary data with specialized service providers who assist us in providing support, technical troubleshooting, and diagnostic services.

These service providers are prohibited from using your Personal Data except for these purposes, and they are required to maintain the confidentiality of your information. In all cases where we share your information in this way, we explicitly require the third-party service providers to acknowledge and adhere to our privacy and data protection policies and standards.

5.2. Marketing Communications

We may share personal data to support marketing communications related to our products and services, mentioned in this Privacy Policy, where you have opted in to receive such communications. This includes sharing limited personal data (e.g., email addresses and user engagement data) with our trusted third-party marketing partners who assist us in delivering relevant content, updates, and promotions. These partners are obligated to handle your data securely and solely for authorized marketing purposes in accordance with applicable privacy laws.

You always have control over your marketing preferences and may opt out of receiving marketing communications at any time by following the unsubscribe instructions in any marketing message or by contacting us directly. We respect your preferences and will promptly honor your request to opt out.

For additional details on how we process data for marketing purposes and share data with marketing partners, please refer to our Privacy Policy for Website Users, which provides more comprehensive information on data use for visitors and website users.

5.3. Legal Disclaimer

We may share your information as required by law, such as to comply with subpoenas, 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.

5.4. Corporate Transactions

If CloudLinux 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.

5.5. Third Parties with Your Consent

We may also disclose your personal information to third parties when you have provided explicit consent. This may include sharing data for specific services or additional functionalities

you wish to access. You will have the option to review and authorize this disclosure before it occurs.

6. HOW WE TRANSFER PERSONAL DATA INTERNATIONALLY

6.1. International Transfer to third parties

This Privacy Policy will apply even if we transfer Personal Data to third parties in other countries. We have taken appropriate safeguards to require that your Personal Data will remain protected wherever it is transferred. When we share the Personal Data of individuals in the European Economic Area ("EEA"), Switzerland, or the United Kingdom ("UK"), we make use of the Standard Contractual Clauses (which have been approved by the European Commission) and the UK International Data Transfer Addendum (as defined within our Data Processing Agreements mentioned in the License Agreements) as well as additional safeguards where appropriate (such as commercial industry-standard secure encryption methods to protect customer data at rest and in transit, TLS for hosted sites, web application firewall protection, and other appropriate contractual and organizational measures). We are also certified to the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), and the UK Extension to the EU-U.S. Data Privacy Framework (UK DPF) Principles to help safeguard the transfer of information we collect from the EEA, Switzerland, and UK. Please see our Data Privacy Framework notice below for more information.

6.2. Data Privacy Framework Notice

Cloud Linux Software, Inc. complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), and the UK Extension to the EU-U.S. Data Privacy Framework (UK DPF) as set forth by the U.S. Department of Commerce. Cloud Linux Software, Inc. has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) concerning the processing of personal data received from the European Union in reliance on the EU-U.S. DPF. Cloud Linux Software, Inc. has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) concerning the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. Cloud Linux Software, Inc. has certified to the U.S. Department of Commerce that it adheres to the UK Extension to the EU-U.S. Data Privacy Framework Principles (UK DPF Principles) concerning the processing of personal data received from the United Kingdom in reliance on the UK DPF. 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 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, CloudLinux is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission (FTC). The Federal Trade Commission has jurisdiction over CloudLinux’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).

Under the Data Privacy Frameworks, EU, Swiss, and UK individuals have the right to obtain our confirmation of whether we maintain personal information relating to you in the United States. Upon request, we will provide you with access to the personal information that we hold about you. You may also correct, amend, or delete the personal information we hold about you. An individual who seeks access, or who seeks to correct, amend, or delete inaccurate data transferred to the United States under Data Privacy Frameworks, should direct their query to privacy@cloudlinux.com. If requested to remove data, we will respond within a reasonable timeframe.

We will provide an individual 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 which it was originally collected or subsequently authorized. To request to limit the use and disclosure of your personal information, please submit a written request to privacy@cloudlinux.com.

In certain situations, we may be required to disclose personal data in response to lawful requests by public authorities, including meeting national security or law enforcement requirements.

Cloud Linux's accountability for personal data that it receives in the United States under the Data Privacy Frameworks and subsequently transfers to a third party is described in the Data Privacy Frameworks Principles. In particular, Cloud Linux remains responsible and liable under the Data Privacy Frameworks Principles if third-party agents that it engages to process the personal data on its behalf do so in a manner inconsistent with the Principles unless Cloud Linux proves that it is not responsible for the event giving rise to the damage.

In compliance with the EU-U.S. DPF, the Swiss-U.S. DPF, and the UK DPF, Cloud Linux Software, Inc. commits to refer unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF, the Swiss-U.S. DPF, and UK DPF to VeraSafe, an alternative dispute resolution provider based in the United States, and the European Union. If you do not receive timely acknowledgment of your DPF Principles-related complaint from us, or if we have not addressed your DPF Principles-related complaint to your satisfaction, please visit VeraSafe Data Privacy Framework Dispute Resolution Procedure for more information or to file a complaint. The services of VeraSafe are provided at no cost to you. More information about VeraSafe, an alternative dispute resolution provider, is provided in section 10(c) below.

ACCESSING OR USING OUR SITES OR SERVICES, OR OTHERWISE PROVIDING INFORMATION TO US OR OUR CUSTOMERS, CONSTITUTES CONSENTING TO OUR POTENTIAL TRANSFER, PROCESSING, AND STORAGE OF SUCH INFORMATION IN THE UNITED STATES.

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 sensitive information is transmitted via Transport Layer Security (TLS) technology to and then stored in our database to be only accessed 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@cloudlinux.com or visit our Security and Compliance web section.

7.2. Retention of Personal Data

How long we keep the information we collect about you depends on the type of information and how we collect and store it. For example, audio and video, in-meeting messages are stored 1 year since the last video call between you and CloudLinux conducted for support services. After a reasonable period, we will either delete or anonymize your information or, if this is not possible, then we will identify your account in our database as “deleted” or “closed” and isolate it from any further use until deletion is possible.

We retain the Personal Data that you provide to us where we have an ongoing legitimate business need to do so (for example, as needed to comply with our legal obligations, resolve disputes, and enforce our agreements).

When we have no ongoing legitimate business need to process your Personal Data, we securely delete the information or anonymize it or, if this is not possible, securely store your Personal Data and isolate it from any further processing until deletion is possible. We will delete this information at an earlier date if you so request, as described in the section "Your Privacy Rights and Choices" below.

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 undergoing processing. For additional copies requested, we may charge a reasonable fee based on administrative costs.
- **Right to rectification:** By 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)**: By 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:
  - fulfilling our legal obligation;

- archival, historical, or scientific research or statistical purposes; or
- determination, exercise, or defense of our legal claims.

- **Right to restriction of processing**: By 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**: By 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 object**: If you have given your consent to the processing of your data by Art. 7 III GDPR, you may revoke your consent at any time in the future. The declaration of revocation must be addressed to us and must be presented in writing or delivered by email or fax.

Please note that to protect Personal Information, we may verify your identity by a method appropriate to the type of request you are making. You are entitled to exercise the rights described above free from discrimination.

We will respond to your request to change, correct, or delete your data within a reasonable timeframe 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.

If you are a customer, prospect, or otherwise interact with a CloudLinux customer who uses our Services and would like to access, correct, amend, or delete your data controlled by the customer, please contact the relevant customer directly. CloudLinux acts as a processor for our customers and will work with our customers to fulfill these requests when applicable.

9. CHILDREN'S ONLINE PRIVACY

CloudLinux 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 under the "How to contact us" Section. We will take appropriate steps to provide access to, correct, or delete the child's data upon verification of your identity.

10. DISPUTE RESOLUTION

Within the scope of this Privacy Policy, if a privacy complaint or dispute relating to Personal Data received by CloudLinux in reliance on the Data Privacy Framework (or any of its predecessors) cannot be resolved through CloudLinux 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/

If a complaint or dispute cannot be resolved through CloudLinux's internal process, we have also agreed to cooperate with the EU and UK data protection authorities and the Swiss Federal Data Protection and Information Commissioner and to participate in the dispute resolution procedures of the panel established by such data protection authorities.

For any dispute arising under the EU-U.S. Data Privacy Framework (DPF) program, the UK Extension to DPF, and the Swiss-U.S. Data Privacy Framework program that is not resolved through the steps described in this section, under certain conditions you may invoke binding arbitration for complaints regarding DPF compliance not resolved by any of the other DPF mechanisms. See more details

https://www.dataprivacyframework.gov/framework-article/ANNEX-I-introduction

11. SUPPLEMENTAL ADDENDUM TO INDIAN RESIDENTS

- **Applicability**

This section applies to Indian residents and outlines our data practices under the India Digital Personal Data Protection Act (DPDPA). For an accessible format of this Privacy Policy, please contact us.

- **How We Collect, Use, and Share Your Personal Information**

We collect, use, and share Personal Data to provide Services as described in this Privacy Policy. Categories of personal data are included in Section 3 of this Privacy Policy.

- **Purposes of Data Processing**

We process your personal data to:

- Provide and maintain our services.
- Communicate about your account and services.
- Fulfill legal obligations and prevent fraud.
- Improve service delivery and user experience.

- **Your Rights Under the DPDPA**

As an Indian resident, you have rights regarding your personal data:

- **Right to Access and Correction**: Request access or correction of your Personal Data.
- **Right to correct:** You may request that we correct inaccurate Personal Information we hold about you.
- **Right to Erasure**: Request deletion of your data when no longer necessary, except where legally required.
- **Right to Withdraw Consent: Withdraw consent for data processing at any time.**

- **Right to Complaint**: File a complaint with our Data Protection Officer or the Data Protection Board of India if your grievance is not resolved satisfactorily.

12. SUPPLEMENTAL ADDENDUM FOR BRAZILIAN RESIDENTS

- **Applicability**

This Supplemental Addendum applies exclusively to residents of Brazil and outlines additional privacy practices and rights under the Lei Geral de Proteção de Dados Pessoais (LGPD). It supplements our existing Privacy Policy.

- **Purpose of Data Processing**

We collect, use, and disclose personal data for the purposes outlined in our primary Privacy Policy. Additionally, per LGPD requirements, we may process your personal data for:

- Compliance with Brazilian laws and regulations
- Protection of credit and legitimate interests in fraud prevention, network, and information security.

- **Legal Basis for Processing**

We process your personal data under the following legal bases as defined by the LGPD:

- Consent (when required for specific data uses);
- Performance of a contract with you;
- Legal or regulatory obligations;
- Legitimate interest, balanced with your rights and freedoms.

You may withdraw consent at any time where consent is the lawful basis for processing, as provided below.

- **Your Rights as a Brazilian Resident**

Under the LGPD, you have specific rights regarding your personal data:

- **Confirmation of Processing**: Request confirmation as to whether we process your personal data.
- **Access**: Request access to your personal data that we hold.
- **Correction**: Request the correction of inaccurate or outdated personal data.
- **Anonymization, or Deletion**: Request anonymization or deletion of unnecessary or excessive personal data.
- **Data Portability**: Request the transfer of your personal data to another service provider, where technically feasible.
- **Information on Data Sharing**: Request information about public and private entities with which we share your data.

- **Withdrawal of Consent**: Withdraw consent for data processing when consent is the legal basis.

13. SUPPLEMENTAL ADDENDUM FOR CANADIAN RESIDENTS

- **Applicability**

This Supplemental Addendum to our Privacy Policy outlines specific provisions for Canadian residents to comply with the Personal Information Protection and Electronic Documents Act (PIPEDA). It applies solely to individuals residing in Canada and supplements the terms in our general Privacy Policy.

- **Collection and Use of Personal Information**

We collect and use Personal Information as outlined in our general Privacy Policy, with additional attention to Canadian legal requirements. Under the PIPEDA, we may only collect, use, or disclose your Personal Information for purposes that a reasonable person would consider appropriate under the circumstances.

We require a lawful basis to process your personal data, which will typically be one or more of the following:

- to fulfill our contractual obligations with you;
- to comply with legal requirements;
- based on your consent, or
- To pursue our legitimate interests, for processing based on legitimate interests, we implement safeguards to ensure these interests do not infringe on your privacy rights and freedoms.

In cases where local law requires us to collect specific personal data, not providing this data could hinder or delay our ability to meet legal requirements and may affect our contractual relationship with you. If we request your consent for processing, you have the right to withdraw it at any time by contacting us through the information provided at the end of this privacy statement.

- **Adherence to the PIPEDA's Principles**

We handle Canadian residents' Personal Information in compliance with the Personal Information Protection and Electronic Documents Act (PIPEDA) by following its 10 Fair Information Principles. We identify and communicate the purpose for data collection, obtain consent when required, and limit the collection and use of information to what's necessary. We maintain data accuracy, implement strong security measures, and ensure transparency about our practices. Canadian residents may access and request corrections to their data, and we welcome any privacy-related concerns, addressing them promptly.

- **Your rights over your Personal Data**

You have certain rights regarding your personal data:

- **Access**: You have the right to request access to the Personal Information we hold about you, including how it is collected, used, and disclosed.
- **Correction**: If you find that your Personal Information is inaccurate, incomplete, or outdated, you have the right to request a correction.
- **Erasure**: You have the right to request erasing or deleting your data.
- **Withdrawal of Consent**: You may withdraw your consent for our collection, use, or disclosure of your personal information at any time, subject to legal or contractual limitations.
- **Challenge Compliance**: If you believe we have not complied with PIPEDA's principles, you can contact our Data Protection Officer to address your concerns. Should your concern remain unresolved, you have the right to file a complaint with the Office of the Privacy Commissioner of Canada (OPC).
- **Right to be Informed**: Individuals have the right to know why their Personal Information is being collected, how it will be used, and if it will be shared with third parties.
- **Data Protection**: We implement safeguards to protect your Personal Information from unauthorized access, disclosure, or misuse.

14. SUPPLEMENTAL ADDENDUM FOR CALIFORNIA RESIDENTS

- **Applicability**

This section applies only to California individuals. 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 arrange to supply 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 Consumer Rights Act ("CCRA").

- **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, fax numbers, physical addresses, and email addresses. We collect this information directly from you or third-party sources.
- Internet or network information, such as browsing and search history. We collect this information directly from your device.
- Geolocation data, such as 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.

- **Sensitive Personal Information**

We do not collect or process any categories of Sensitive Personal Information as defined under the California Consumer Rights Act (CCRA). In the event this practice changes, we will update this Privacy Policy and provide appropriate notice to ensure compliance with applicable laws.

- **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 limit the use of Sensitive Personal Information**: You may request to limit our use of your Sensitive Personal Information to specific business purposes.
- **The right to opt-out of sharing or selling**: While CloudLinux does not sell Personal Information to third parties, the CCRA 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.

CloudLinux 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).

15. USE OF THE AUTOMATED MAKING DECISION TOOL

We are committed to transparent and secure handling of your personal information. We do not use artificial intelligence (AI) or automated decision-making processes that produce legal effects concerning you or otherwise significantly impact you. All decisions related to the processing, storage, and protection of personal data are made with human involvement, in accordance with our established privacy and security policies.

Automated decision-making occurs when an electronic system uses personal data to make decisions without human involvement. Under applicable data protection laws, you have the right not to be subject to decisions based solely on automated processing that have legal effects

or significantly affect you. Should you have any concerns or require clarification, you are entitled to request the involvement of one of our representatives in any decision-making process related to your data.

If our approach to AI usage changes, we will promptly update this Privacy Policy to reflect new practices and ensure that you are informed.

16. CHANGES TO THIS PRIVACY POLICY

We may update this Privacy Policy from time to time. We will notify you of any changes by posting the new Privacy Policy on our website with a new effective date. We encourage you to review this policy periodically for any updates.

17. 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:

Cloud Linux Software, Inc.
Email: privacy@cloudlinux.com