Siinc Privacy Policy

Last Updated: 12 January 2026

Effective Date: 12 January 2026

1. Introduction and Scope

Welcome to Siinc. This Privacy Policy describes how Siinc Pty Ltd and its global affiliates ("**Siinc**," "**we**," "**us**," or "**our**") collect, use, disclose, secure, and otherwise process Personal Data. This policy is designed to be comprehensive and to comply with data protection laws in the jurisdictions where we operate, including Australia, the United Kingdom, the European Economic Area, and the United States.

This Privacy Policy applies to Personal Data we collect when you:

- Visit our website, https://www.siinc.io (the "**Website**");
- Register for, access, or use our data backup and synchronisation services (the "**Services**");
- Interact with us in the context of our other business activities, such as marketing campaigns, sales enquiries, events, and customer support.

By accessing our Website or using our Services, you acknowledge that you have read and understood this Privacy Policy. This policy should be read in conjunction with our End-User Licence Agreement ("**EULA**").

2. Definitions

For the purposes of this Privacy Policy:

"Personal Data" means any information that relates to an identified or identifiable individual. This may include, but is not limited to, name, email address, IP address, or payment information.

"Processing" means any operation or set of operations which is performed on Personal Data, such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, disclosure, or erasure.

"Data Controller" means the entity that determines the purposes and means of the Processing of Personal Data.

"Data Processor" means the entity that Processes Personal Data on behalf of the Data Controller.

"GDPR" means the General Data Protection Regulation (EU) 2016/679.

"UK GDPR" means the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

"CCPA/CPRA" means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020.

SIINC

3. Our Role: Data Controller and Data Processor

It is crucial to understand our role concerning your data. Depending on the context, we act as either a "Data Controller" or a "Data Processor."

3.1. Siinc as Data Controller. We act as a **Data Controller** when we determine the purposes and means of processing Personal Data for our own business needs. This includes:

- **Account and Commercial Data:** Personal Data you provide when you create an account, request a trial, or purchase a subscription (e.g., your name, email, company name, billing information).
- **Website and Marketing Data:** Personal Data collected automatically when you visit our Website (e.g., IP address, cookie data) or that you provide when you interact with our marketing initiatives (e.g., downloading a whitepaper).
- **Communication Data:** Personal Data related to our communications with you (e.g., support queries, feedback).
-

This Privacy Policy primarily governs our processing activities as a Data Controller.

3.2. Siinc as Data Processor. We act as a **Data Processor** when we process data on behalf of our customers in the course of providing our Services. Our Services are designed to back up and synchronise data from our customer's Autodesk Construction Cloud account ("**Customer Data**") to a storage location controlled by the customer ("**Customer Storage**").

- In this capacity, our customer is the Data Controller. The customer is responsible for the lawfulness of the processing of Customer Data, including any Personal Data it may contain.
- Our processing of Customer Data is governed by our EULA and, where applicable, a Data Processing Addendum ("**DPA**") with our customer.
- We only process Customer Data in accordance with our customer's lawful, documented instructions to provide, secure, maintain, and monitor the Services. We do not access, use, or disclose Customer Data for our own purposes, such as advertising or marketing.
- If you are an individual whose Personal Data is contained within a Siinc customer's Customer Data and you have questions or wish to exercise your data protection rights, please direct your enquiry to the relevant Siinc customer (the Data Controller).

4. Personal Data We Collect (as Data Controller)

We collect Personal Data from various sources:

4.1. Information You Provide Directly

- **Account and Profile Information:** When you create an account, sign up for a free trial, or purchase our Services, we collect your first and last name, email address, phone number, company name, job title, and password.
- **Payment and Billing Information:** When you purchase a subscription, we collect payment and billing information, such as billing address and payment card details. This information is securely processed by our third-party payment processors (e.g., Stripe). We do not store your full payment card details on our servers.
- **Communications and Support:** When you contact our sales or support teams, participate in a survey, or otherwise communicate with us, we collect your name, contact details, and the content of your communications.

- **Marketing and Events Information:** When you subscribe to our newsletter, download content (like a whitepaper), or register for a webinar or event, we collect your name, email address, and professional information such as your company and job title.

4.2. Information We Collect Automatically

- **Log and Usage Data:** When you use our Website or Services, our servers automatically record information, including your Internet Protocol (IP) address, browser type and settings, device information, operating system, referring URLs, pages visited, access times, and crash data.
- **Cookies and Similar Technologies:** We use cookies, web beacons, pixels, and similar technologies to operate and improve our Website and Services, analyse performance, understand user activity, and for marketing purposes. For more details, please see Section 12 ("Cookies and Tracking Technologies").

4.3. Information from Third-Party Sources

- **Authentication Services:** You connect to our Services using OAuth for Autodesk Construction Cloud. When you authenticate, we receive a security token to access your account data on your behalf. We do not receive or store your password for your Autodesk account.
- **Analytics Providers:** We receive aggregated information and analytics about user interaction with our Website and marketing campaigns from third-party analytics providers like Google Analytics.
- **Publicly Available Sources:** We may collect information from publicly available sources, such as professional networking sites (e.g., LinkedIn), to identify potential business customers.

5. How We Use Your Personal Data and Our Legal Basis for Processing

We use the Personal Data we collect as a Data Controller for the purposes outlined below. If you are in the European Economic Area (EEA) or the United Kingdom (UK), we also identify the legal basis for processing.

Purpose of Processing	Categories of Personal Data Used	Legal Basis (EEA/UK)
To Provide, Manage, and Secure the Services. To set up and maintain your account, process payments, provide the core backup and synchronisation functionality, authenticate users, and fulfil our contractual obligations under the EULA.	Account and Profile Information, Payment and Billing Information, Log and Usage Data.	**Performance of a Contract.**
To Communicate with You. To send you service-related announcements (e.g., maintenance, security alerts), respond to your enquiries, and provide customer support.	Account and Profile Information, Communications and Support Data.	**Performance of a Contract; Legitimate Interests** (to provide effective support).

To Improve and Develop Our Services. To analyse usage trends, gather feedback, conduct research, and enhance the functionality, security, and user experience of our Website and Services.	Log and Usage Data, Communications and Support Data, Analytics Data.	**Legitimate Interests** (to improve our commercial offering).
For Security, Compliance, and Fraud Prevention. To protect our Services and users, prevent and detect fraud, enforce our legal terms, and comply with our legal and regulatory obligations.	Account and Profile Information, Log and Usage Data, Payment and Billing Information.	**Legal Obligation; Legitimate Interests** (to protect our business and users).
For Marketing and Promotions. To send you marketing communications about our products, services, and promotions that may be of interest to you.	Account and Profile Information, Marketing and Events Information, Cookies Data.	**Consent** (where required by law); **Legitimate Interests** (to market our services to existing customers or business contacts).

6. Data Sharing and Disclosure

We do not sell your Personal Data. We may share your Personal Data with the following categories of third parties, only as necessary for the purposes described in this policy:

- **Service Providers (Sub-processors):** We engage third-party companies to perform services on our behalf, such as cloud hosting (e.g., AWS, Azure), payment processing, customer relationship management (CRM), marketing automation, and analytics. These providers are contractually obligated to protect your data and are only permitted to use it to provide services to us.
- **Affiliates:** We may share information with other companies in the Siinc corporate group for operational purposes, such as providing support and developing services, consistent with this Privacy Policy.
- **Professional Advisors:** We may share your Personal Data with our lawyers, accountants, insurers, and other professional advisors as necessary to obtain advice or otherwise protect and manage our business interests.
- **Business Transfers:** In the event of a merger, acquisition, bankruptcy, reorganisation, or sale of all or a portion of our assets, your Personal Data may be transferred as part of that transaction. We will notify you via email and/or a prominent notice on our Website of any change in ownership.
- **Legal Requirements:** We may disclose your Personal Data if required to do so by law, subpoena, or in the good faith belief that such action is necessary to (a) comply with a legal obligation or government request, (b) protect and defend our rights or property, (c) prevent or investigate possible wrongdoing in connection with the Services, or (d) protect the personal safety of users or the public.
- **With Your Consent:** We may share your information with other third parties with your explicit consent.

7. International Data Transfers

Siinc is a global company with offices in Australia, the United States, the United Kingdom, and Singapore. Your Personal Data may be transferred to, and processed in, countries other than the country in which you are resident. These countries may have data protection laws that are different from the laws of your country.

Specifically, our primary servers are located in, Australia, USA, Europe, and our global teams and service providers operate around the world. This means that when we collect your Personal Data, we may process it in any of these countries.

SIINC

Where we transfer Personal Data from the EEA, UK, or Switzerland to other countries not deemed to provide an adequate level of data protection, we do so on the basis of appropriate legal safeguards. These safeguards may include the European Commission's Standard Contractual Clauses (SCCs) and/or the UK's International Data Transfer Addendum (IDTA), along with supplementary measures as required, to ensure your Personal Data receives an adequate level of protection.

8. Data Security

We have implemented and maintain appropriate administrative, technical, and physical security measures designed to protect the security, confidentiality, and integrity of your Personal Data from unauthorised access, use, or disclosure. These measures include:

- Encryption of data in transit (using TLS) and at rest (using AES-256).
- Strict access controls based on the principle of least privilege to ensure only authorised personnel can access Personal Data.
- Regular security assessments, vulnerability scanning, and penetration testing.
- A formal incident response plan.
- Regular data protection and security training for our staff.

You are responsible for maintaining the security of your account credentials. While we take security seriously, no security measures are perfect or impenetrable, and we cannot guarantee the absolute security of your data.

9. Data Retention

We will retain your Personal Data only for as long as is necessary to fulfil the purposes for which it was collected, and for as long as required to satisfy any legal, accounting, or reporting requirements. To determine the appropriate retention period for Personal Data, we consider:

- **Ongoing Relationship:** The duration of our business relationship with you (e.g., for as long as you have an active account with us).
- **Legal Obligations:** Whether there is a legal or regulatory obligation to which we are subject (e.g., tax and corporate laws require us to keep transaction records for a certain period).
- **Legal Position:** Whether retention is advisable in light of our legal position (e.g., regarding applicable statutes of limitations, litigation, or regulatory investigations).
- **Purpose:** The amount, nature, and sensitivity of the Personal Data and the purpose for which we process it.

When we no longer have a legitimate business need to process your Personal Data, we will either delete or anonymise it, or, if this is not possible (for example, because your Personal Data has been stored in backup archives), then we will securely store it and isolate it from any further processing until deletion is possible.

10. Your Data Protection Rights

Depending on your location and subject to applicable law, you may have certain rights regarding your Personal Data. We are committed to upholding these rights for all our users. To exercise any of these rights, please contact our Privacy Officer at get@siinc.io. We will

respond to your request in accordance with applicable data protection laws. We may need to verify your identity before processing your request.

10.1. Rights for Residents of the EEA and UK. If you are a resident of the EEA or the UK, you have the following rights under GDPR and UK GDPR:

- **Right of Access:** To request a copy of the Personal Data we hold about you.
- **Right to Rectification:** To request that we correct any inaccurate or incomplete Personal Data.
- **Right to Erasure ('Right to be Forgotten'):** To request that we delete your Personal Data, under certain conditions.
- **Right to Restrict Processing:** To request that we restrict the processing of your Personal Data, under certain conditions.
- **Right to Data Portability:** To request that we transfer the data that we have collected to another organisation, or directly to you, in a structured, commonly used, and machine-readable format.
- **Right to Object:** To object to our processing of your Personal Data, particularly where we rely on legitimate interests as our legal basis, or for direct marketing purposes.
- **Rights in Relation to Automated Decision Making and Profiling:** You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or similarly significantly affects you.
- **Right to Withdraw Consent:** Where we rely on your consent to process your Personal Data, you have the right to withdraw that consent at any time.
- **Right to Lodge a Complaint:** You have the right to lodge a complaint with your local supervisory authority.

10.2. Rights for Residents of Australia. Under the Australian Privacy Act 1988, you have the right to access the personal information we hold about you and to request its correction. You also have the right to make a complaint to the Office of the Australian Information Commissioner (OAIC) if you believe your privacy has been breached.

10.3. Rights for Residents of the United States. Several U.S. states have enacted comprehensive privacy laws. If you are a resident of California, Virginia, Colorado, Connecticut, Utah, or another state with an applicable privacy law, you may have the following rights, subject to certain exemptions:

- **Right to Know and Access:** The right to know what personal information we have collected, used, and disclosed about you, including the categories of information, sources, purposes of collection, and categories of third parties to whom we have disclosed it. You may also request a copy of the specific pieces of personal information we have collected about you.
- **Right to Delete:** The right to request the deletion of your personal information that we have collected, subject to certain exceptions (such as to complete a transaction or to comply with a legal obligation).
- **Right to Correct:** The right to request the correction of inaccurate personal information that we maintain about you.
- **Right to Opt-Out of Sale or Sharing for Cross-Context Behavioural Advertising:** Siinc does not "sell" personal data in the traditional sense of exchanging it for monetary consideration. However, under some laws, our use of cookies for analytics or targeted advertising may be considered a "sale" or "sharing". You have the right to opt-out of this activity. You can exercise this right by managing your cookie

preferences as described in Section 12 or by enabling a Global Privacy Control (GPC) signal in your browser.

- **Right to Limit Use of Sensitive Personal Information (SPI):** We do not collect or process SPI for the purpose of inferring characteristics about you.
- **Right to Non-Discrimination:** We will not discriminate against you for exercising any of your privacy rights, such as by denying you services or charging you different prices.

Exercising Your US Rights: To exercise these rights, please contact us at get@siinc.io.

You may also designate an authorised agent to make a request on your behalf.

Specific Information for California Residents (CCPA/CPRA): In the preceding 12 months, we have collected the categories of personal information listed in Section 4 from the sources described therein. We collect this information for the business and commercial purposes described in Section 5 and disclose it to the categories of third parties listed in Section 6. California's "Shine the Light" law (Civil Code Section § 1798.83) also permits users of our Website that are California residents to request certain information regarding our disclosure of personal information to third parties for their direct marketing purposes. To make such a request, please contact us.

11. Cookies and Similar Tracking Technologies

We use cookies and similar tracking technologies (like web beacons and pixels) to track activity on our Website and hold certain information. Cookies are small data files stored on your device that help us to operate our Website, understand how you use it, and personalise your experience.

We categorise our cookies as follows:

- **Strictly Necessary Cookies:** These are essential for the Website to function and cannot be switched off. They are usually only set in response to actions made by you which amount to a request for services, such as setting your privacy preferences or filling in forms.
- **Performance and Analytics Cookies:** These cookies allow us to count visits and traffic sources so we can measure and improve the performance of our site. They help us to know which pages are the most and least popular and see how visitors move around the site.
- **Functionality Cookies:** These cookies enable the Website to provide enhanced functionality and personalisation. They may be set by us or by third-party providers whose services we have added to our pages.
- **Targeting and Advertising Cookies:** These cookies may be set through our site by our advertising partners. They may be used by those companies to build a profile of your interests and show you relevant adverts on other sites.

Managing Your Preferences: Where required by law, we will ask for your consent before placing non-essential cookies on your device. You can manage your preferences at any time through our cookie consent management tool on our Website. You can also instruct your browser to refuse all cookies or to indicate when a cookie is being sent. However, if you do not accept cookies, you may not be able to use some portions of our Service.

12. Children's Privacy

Our Services are intended for business use and are not directed to individuals under the age of 18. We do not knowingly collect Personal Data from children under 18. If we become

aware that a child under 18 has provided us with Personal Data, we will take steps to delete such information from our files.

13. Third-Party Links

Our Website may contain links to other websites that are not operated by us. If you click on a third-party link, you will be directed to that third party's site. We have no control over and assume no responsibility for the content, privacy policies, or practices of any third-party sites or services. We strongly advise you to review the privacy policy of every site you visit.

14. Changes to This Privacy Policy

We may update our Privacy Policy from time to time to reflect changes in our practices or for other operational, legal, or regulatory reasons. We will notify you of any material changes by posting the new Privacy Policy on this page and updating the "Last Updated" date at the top. We may also provide notice to you through your account or via email. You are advised to review this Privacy Policy periodically for any changes.

15. Contact Us

If you have any questions, comments, or concerns about this Privacy Policy or our data practices, or if you wish to exercise your rights, please contact our Privacy Officer:

Siinc Pty Ltd
Attn: Privacy Officer
Email: get@siinc.io

Registered Address: Level 35, Tower One Barangaroo100 Barangaroo Avenue
Sydney NSW 2000Australia

Representatives for Data Subjects in the EU and UK:

For the purposes of Article 27 of the GDPR and UK GDPR, we have appointed the following representatives:

EU Representative:

UK Representative: