Rendra AS Privacy Notice

Revised: 06 May 2025

This Privacy Notice (“Notice”) for Rendra AS (company reg. no. 898 353 672, head office: Østre Aker vei 17, 0581 Oslo, Norway, hereinafter referred to as “RENDRA”, “we” “us” and “our”) and including its subsidiary StreamBIM Japan Co.,Ltd., explains how we, concerning data protection collect, share, and process personal data as data controllers, when you:

- Visit our website at https://www.streambim.com (“Website”)
- Register to use our services, including the services available through our Website, our mobile and browser applications (collectively referred to as “Services”)
- Register and/or attend our webinars and events, like StreamBIM Day
- Contact us for Sales or Support by telephone, email or web form

RENDRA endeavours to ensure that all legal requirements and obligations to protect your personal data subject to the Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (“GDPR”) are met. The references to “personal data” and “personal information” have the same meaning under this Notice and refer to any information that directly or indirectly can be linked to an identifiable natural person (“you”).

If you have chosen to use servers located outside of the EU/EEA area, we are in addition subject to the following data privacy legislation:

Japan server:	The Act on the Protection of Personal Information Act No. 57 of 2003 (“APPI”) (個人情報の保護に関する法律、平成15年5月30日法律第57号)
Australia server:	Privacy Act 1988 (Cth)

This Notice also describes your privacy rights. If you have agreed to any of our applicable terms and conditions that govern the use of any of our Services, those terms and conditions are thus incorporated to this Notice accordingly with reservations to any individually agreed terms and conditions between us and you. Please read this Notice and our terms and conditions thoroughly before using our Website and Services, in order to ensure that you fully understand our views and practices on handling and processing your personal data, and on what terms and conditions we provide you our Services.

We strive to protect and respect your personal data to the best of our ability. Please be aware, that when you access or agree to use our Website and/or Services, you unconditionally acknowledge, agree, and accept the terms in this Notice.

If you use the our Services as part of an entity, corporation or non-profit organisation (collectively, ‘Organisation’) that has entered into an agreement with RENDRA, the terms of the agreement between the Organisation and RENDRA will supersede this Privacy Policy in the event of any conflict.

1. Please be aware that this Notice does not apply to:

1.1 Customer-supplied data

Except for the user account information (as described below), this Notice does not apply to our privacy practices in relation to Customer-owned materials uploaded and stored in our Services by you as an end user or by your employer or other project stakeholders (“Customer Data”), such as drawings, images, BIM files, messages and any other electronic data. RENDRA processing in regard to Customer Data are instead governed by the Contract and the Data Processing Agreement, which

regulates the agreement between you or the Organisation and RENDRA regarding access to- and use of our Services.

RENDRA is only responsible for ensuring compliance with applicable laws and regulations related to the collection, use, and storage of personal information in connection with our Services, for which we collect directly.

1.2 Third Parties, links and StreamBIM integrations

Our Website and Services may contain links or integrate with other websites and online services. RENDRA is not responsible or liable for any damage or loss related to your use of any third-party websites or online services. Please refer to the terms and privacy policy of the relevant third-party websites and online services before using them, whether directly or in connection with your use of the Website and/or Services.

2. How RENDRA collects your personal data

We collect and aggregate your personal data in various ways. It can be collected either directly from you, by the use of cookies and other tracking technologies, automatically collected or generated when you interact with and use our Website and/or Services or collected when provided by third parties.

2.1 Data Collected from you

We collect and process your personal data from you directly when you sign up to create an account to use our Services, register for any of our webinars and events, interact with us on social media, and/or when you provide us with personal information by contacting us directly via email or web form.

We may collect the following categories of information directly from you:

- Identification information. We may collect data such as given and family names, telephone number, email, and company/employer.
- User profile information. When you sign up for a test project and/or create a user account, we collect your given and family names, phone number, email address, preferred language, and company/employer.
- Support cases. We may also collect information in connection with a support activity when you use the app-integrated support chat or email us.

- Attendee information. When you register and/or attend a webinar or event hosted by RENDRA, we may collect personal information such as given and family, phone number, email address, and company/employer.
- Billing information. When you subscribe to our Services, RENDRA collects financial information to send you invoices and other relevant communication.

2.2 Data gathered when you use our Website and Services

When visiting our Website and using our Services we use different ways of collecting information about you that is necessary to use the full range of our Services, as well as information that helps us improve your user experience.

We use “cookies”, a small amount of anonymous information, to store some relevant session information. We may store and access such “cookies” on your device.
We may also use web beacons (clear GIFs) to collect information such about your interaction with our HTML marketing emails and newsletters that you subscribe to, e.g. if you have opened or clicked on a link. When using our Services, we may also collect device and usage information. Device related information may be IP addresses, browser used, various device specifications and location information. Usage information may be a behavioural pattern when using our Website and/or Services.

2.3 Data gathered via integrated services

If you are given the option to access the Services through the use of SSO (Single Sign-On), username and passwords provided by third parties or Integrated Services, e.g. Microsoft Azure, you authorise the Integrated Service to provide personal information to RENDRA. You are responsible to review the privacy notices and terms of use for each Integrated Service that you engage with prior to connecting to our Services. Please contact the SSO provider for more information regarding their privacy policies.

2.4 Data provided to us by third parties

We may store and collect personal information about you from third-party sources, such as resellers or other affiliates and business partners, publicly available sources and registers, and social networking platforms such as LinkedIn or Facebook. The categories of personal data we may collect about you from third-party sources include professional information, such as your occupation, field of industry,

employment history, work experience, educational background, and other qualifications, or identification information such as given name, last name, telephone number, email, and company/employer.

We may combine the personal information we receive directly from you, collected by us, or received by third parties when allowed to do so in accordance with applicable laws, for the purpose of providing you with relevant content, experiences, and other offerings, as well as for keeping our records updated with accurate information about you.

3. How RENDRA uses your personal data

We use the personal data we have collected about you for various purposes listed below, as long as we have secured a lawful ground for processing.

3.1 When deemed contractually necessary

- To process and complete your registrations via our Website or when using our Services.
- To perform our obligations and deliveries subject to a contract with you or your employer or to validate your identity when entering a contract with you. This includes audit trails after your user has been made inactive on the project.
- To provide you with our Services, including support and direct communication.
- To send information to you within the scope of our contract. This may be to send you service messages, inform you of new updates, releases, errors, and other relevant information relating to the use of our Services such as changes to our Terms and Conditions.
- To perform any financial activity, such as invoicing.
- To provide feedback and information to requests or queries.

3.2 When based on a valid interest of RENDRA (or a third party)

- To provide information about upcoming events (including webinars) related to the support or use of our products or to follow up on completed RENDRA events.
- To improve the quality, functionality and user experience of our products and services, including analysing how they are being used.

- Automated analytic systems and other tracking techniques may be used to fulfil this purpose (if not subject to your consent).
- To uphold and maintain the security on our Website and Services by detecting, mitigating, and preventing security threats, perform maintenance, and debugging.
- To enforce our terms and conditions when using our Services.
- Other activities relating to the protection of your, our or any third-party rights, property, and safety.
- To anonymise, aggregate, or perform other non-identifying purposes in relation to your personal data.
- To manage existing and potential customer relationships.

Please note that you have the right to object to our processing of your personal data when we rely on a legitimate interest for the processing. Please refer to the “Your Rights” section in chapter 7.

3.3 When you have given your consent

- To send you relevant marketing materials such as promotional offers and advertising.
- To share information about you with third parties (listed data handlers and sub-processors).
- To use cookies or similar technologies.
- To send push notifications to your mobile device.
- To send email notifications.
- To perform various legitimate processing activities.

The consent for processing that you have given us you are entitled to withdraw at any time. Please contact us if you wish to withdraw your consent. Please also note that some data retention may still be required for contractual or legal reasons, as described below.

3.4 When required to fulfil a legal obligation

- To respond, disclose, or share your personal data with relevant authorities following an official request.

4. Who does RENDRA share your personal data with?

We share the collected information about you with the following parties when relevant:

- Our service providers, who perform services or certain functions on our behalf, for example companies supporting us with invoicing, licences, software maintenance, hosting, user verification and localization, marketing, security, support, analytics, social media etc. Please note that all service providers who we may share your personal information with are subject to a contract that either restricts or limits their ability to process and use your personal information.
- Other relevant third parties in connection with a business transaction, hereunder a transfer, outsourcing, merger, sale, acquisition, consolidation, change in control, reorganisation, or liquidation of RENDRA, or parts hereof.
- Legal circumstances, when we are required to do so by law, e.g. following a court order, or when we otherwise in good faith believe that it is required by law or with the law enforcement or other reasonable persons. An example of this would be a legal counsel or external lawyer, when we believe that a submission of the personal information is necessary to identify, contact and prevent, or respond to fraud and/or an intellectual property right infringement caused knowingly or unknowingly for the purpose of protecting RENDRA's intellectual property rights and security.
- Administrators and other end users in your organisation, who may gain access to your personal information when you accept an invitation to join a project or building on behalf of your organisation or enterprise.
- Project members through the members list, depending on privilege.
- Any other person with your consent to the disclosure.

5. Location of personal data storage and cross-border transfers

RENDRA transfers personal data to some of our third parties described above in the section: "Who does RENDRA share your personal data with?" to help fulfil our obligations towards you, for example to provide a secure storage of your data, hosting and support. As an underlying basis, RENDRA aims to only engage sub-processors or third parties where the processing and storage of personal data remains within the EEA. When it is not possible, RENDRA relies on the following legal mechanisms to ensure the same level of protection as guaranteed by the

GDPR when transferring personal data to third parties outside of the EEA: Third countries deemed adequate by the European Commission, appropriate safeguards e.g. Standard contractual clauses (SCC) adopted by the European Commission, approved binding corporate rules (BCR) or any other current or future appropriate safeguards pursuant to Article 46 of the GDPR, or your explicit consent.

If there are any material changes to the way that customer data is processed, the changes will be communicated to all customers and users, and prior approval obtained wherever applicable.

6. How does RENDRA protect your personal data?

The protection and security of your personal data is a fundamental consideration at RENDRA, and is governed by our ISO 27001 certified Information Security Management System (“ISMS”). We work to maintain various technological, administrative, and physical measures to protect your personal data from unauthorised surveillance and access and malicious actions. We also take reasonable steps to limit the sharing and access of your personal data to only concern employees and contractors who need access to your data to perform a contract or other relevant function.

7. Your rights

You have the right to access the personal data we process about you, with the exceptions set out in the GDPR and other applicable laws. You also have the right to object to our processing our use of your personal data, to rectify your personal data, and require us to limit the processing of your personal data.

If we process personal data based on your consent, you have the right to withdraw this consent at any time. If you withdraw your consent, we will stop processing your personal data, unless continuation of processing is necessary to comply with our legal and/or contractual obligations, as required or permitted by law.

If you request us to delete the personal data we have registered about you, we will do so without undue delay unless we can continue the processing pursuant to a different legal basis, such as a legal obligation to store and keep your personal data. If you are an individual user subject to a contractual arrangement with any of our

customers (e.g. your employer or their customer) which includes the processing of your personal data on behalf of said customer, we may refer any enquiry by you to the customer and cooperate with their handling of your enquiry, in order to comply with our contractual obligations towards the customer.

If you wish to exercise any of your applicable rights as described above, please contact us. We will respond to your inquiry as soon as possible.

8. Notice to end-users regarding products provided by your organisation

Our Services are intended for use by organisations and enterprises. Please note that when our Services are made available to you through an enterprise customer of RENDRA's (i.e. your employer or their customer), that organisation or enterprise is the data controller of your personal information within our Services, which in turn we collect to create a user profile with us. RENDRA is not responsible for the privacy or security practices of that organisation, which may differ from the practices that are described in this Notice.

As an end-user, you may be using our Services on behalf of an organisation you are affiliated with, such as your employer or school affiliation. Please note that through project administrators, your organisation can:

- Control and administer your use of our Services
- Access and process your personal data, including the interaction data and contents of the files you have uploaded to a project via our Services

9. Data retention

In cases where RENDRA is the data controller of personal information as described above, we will keep your personal data for as long as we need it to fulfil any of the purposes described under the section: "How RENDRA uses your personal data", to the extent we can do so lawfully. This includes our right to store your personal data longer if we must do so in order to comply with a legal or contractual obligation, even if the original purpose for processing your personal data can no longer be justified. When we no longer have any justified legitimate needs to retain your data, your data will be anonymized or deleted.

Please note that in order to preserve a full audit trail, user profiles cannot be completely removed from a project database until the project itself has been deleted. If your user account is registered in a log of performed actions (topic comment, approved checklist point, etc.), this log is a legal requirement for documentation purposes, and your personal information will be stored in our database for the duration of the project period, or as long as it is deemed necessary by the project owner. Users can be set as inactive to remove access to a project.

When all projects containing these logs are terminated and deleted from the StreamBIM database, your personal information with regard to these records will also be automatically deleted.

When we use your personal data in connection with marketing purposes by your consent, we will use your personal information until you withdraw your consent. Please be aware that it will be necessary for us to store the registered information about your not wanting to receive marketing materials from us if you have decided to withdraw your consent.

10. Children's privacy

Our Website and Services and their contents are not directed towards children who are under the age of 16. If we unknowingly happen to collect personal data from children or minors, any information provided by a child or minor to RENDRA or its service providers without parental consent will be deleted as soon as it is discovered. If you have any questions or knowledge about personal data that may have been submitted by a minor, please contact us.

11. Contact information

If you have any questions, requests or concerns relating to this Notice or if you wish to exercise any of your rights described above, please contact us by the **in-app support chat** or by **email** to: office@rendra.io.

When contacting us, please inform us of which RENDRA Service your enquiry concerns as well as your full name and email-address, so that we can identify you and process your enquiry or request. We may ask for additional forms of verification depending on the nature of the inquiry and personal information requested.

If you have any complaints regarding the processing of your personal data or this Notice, we will cooperate with you to find a satisfactory resolution to your matter. If you believe that we have not assisted you sufficiently or have acted in breach of your rights, you have the right to file a complaint to *Datatilsynet*, the Norwegian supervisory authority (Postal address: Postboks 458 Sentrum, 0105 Oslo, Norway), or to another competent European Supervisory Authority or equivalent subject to your location.

12. Updates to this Notice

RENDRA may change or update this Notice when necessary. We will announce any changes by updating the date, as stated on the top of this Notice. Please review this Notice regularly to make sure you are up to date with the latest version published.