## Rendin OÜ Privacy Policy v1.4 effective from 15.05.2026

The principles of processing user data provide an overview and explain how Rendin OÜ processes (collects, processes, and shares) personal data collected during the use of its services and platform. Rendin OÜ (registry code: 14672861) operates as the data controller and manages the Rendin platform (an environment created by Rendin, including the website and mobile application). Our contact details are Peterburi tee 2f, Tallinn, Harjumaa, 11415. For questions regarding data protection and personal data processing, please contact us via email at **info@rendin.co**.

Our users are visitors to the Rendin platform, as well as parties to rental agreements and contract managers (e.g., agents) who can input data, create and manage rental agreements, report incidents, and exchange information with Rendin.

The insurance service provider is PZU Insurance (legal name: AB „Lietuvos draudimas“ Estonian Branch).

### I What information do we collect?

The information collected is necessary for providing the relevant service and fulfilling our legal obligations. Users may choose not to share their information with Rendin, but this will limit full access to the service.

We ask for and collect the following personal data during the use of the platform and service:

1. **Information entered by the user on the platform:**
   - 1.1. Personal details, including first and last name, date of birth, personal identification number, and ID document details.
   - 1.2. Contact details, including email address, phone number, address, communication language, and residential address.
   - 1.3. Communication between Rendin and the user.
   - 1.4. Other information the user decides to share, such as gender, access to device data, or photos.
2. **Information collected automatically:**
   - 2.1. Technical data, which may include IP address, device, software, and similar information.
   - 2.2. Social network data, which may include identification and social account information.
   - 2.3. Payment information, including relevant details of any payment transactions on the platform (Rendin does not store card information).
   - 2.4. Cookies (see the "Cookies" section for more details).
3. **Calls and chats:** Users are notified of recordings at the beginning of a call. Recorded calls and emails, Facebook Messenger conversations are used to improve service quality and resolve disputes.
4. **Information obtained from third parties:** Rendin does not control or take responsibility for methods third parties use to collect information. Questions regarding such information should be directed to the third party. This includes:
   - 4.1. Publicly available information, such as social networks and public databases.
   - 4.2. Information obtained from Rendin's partners.
   - 4.3. Data from credit default registers.

### II How does Rendin use User information?

1. Rendin uses user information in the following ways:
   - 1.1. To fulfill contractual obligations and provide information related to products and

services, including sharing necessary data with the insurance provider PZU Insurance to offer the best possible deals and issue insurance certificates.

1.2. To comply with legal and/or regulatory obligations to ensure the safety and security of products.

1.3. To notify users of changes to Rendin's service terms and offers.

1.4. To support internal processes and service administration (e.g., troubleshooting, data analysis, testing, research, and statistics).

1.5. To collect statistics and analytics for improving the service.

1.6. To measure, understand, and improve the effectiveness of marketing (see the "Marketing" section for more details).

1.7. To provide information about other similar services and offers by Rendin.

1.8. To combine user-provided information with information from other sources for the above purposes.

2. Sharing personal data with third parties:

2.1. If required by law or to protect the rights, property, or safety of Rendin or its users. This may include sharing information with other companies for credit and background checks, as well as detecting fraud or other illegal activities when there is sufficient basis.

2.2. For assessing credit or insurance risks.

2.3. For issuing an insurance certificate.

**III Restriction of Access and Risk Management**

1. Rendin has the right to apply risk-based measures, including restricting or prohibiting a person’s access to the platform and adding the person to a restricted access list, where necessary to protect Rendin’s legitimate interests, the security of contractual relationships, or compliance with legal obligations.
2. A decision to restrict access may, among other things, be based on:

2.1. previous contractual relationships in which breaches, outstanding debts, or other failures to fulfill obligations have occurred;

2.2. violations of the platform’s terms of use, codes of conduct, or the principle of good faith;

2.3. Rendin’s risk assessment, including cases where there has been no prior contractual relationship with the person, but there is an increased risk of non-performance of contractual obligations or potential damage.

3. Rendin has the right to retain, to the minimum extent necessary, personal data in the restricted access list (e.g., personal identification code), including in cases where the person has requested deletion of their account, for the purpose of:

3.1. preventing the conclusion of new contracts with a Rendin guarantee;

3.2. protecting its legitimate interests and preventing fraud or damage.

4. Personal data is retained only to the extent necessary to achieve the above purposes.
5. Decisions on access restriction are reviewed:

5.1. upon a reasoned request from the person; or

5.2. periodically, but no later than 5 years from the date of the decision, unless a longer retention obligation arises from applicable law.

**IV How does Rendin store User information?**

Rendin processes and securely stores user data on servers located within the European Union. When using third-party tools, Rendin ensures that all tools comply with applicable data protection requirements and the General Data Protection Regulation (GDPR). Rendin retains user data for up to five years after the end of the user relationship and transaction and contract information for ten years. After this period, user data and files are deleted from the databases.

## V Marketing

Rendin aims to provide users with product and service information deemed relevant. Users can opt out of receiving such information at any time by notifying Rendin via the platform or email at info@rendin.co.

1. **Data collection and usage purposes:**
   1.1. Rendin collects data from the web platform, mobile application, and via the server to provide the User with relevant and effective advertisements, as well as to improve our services and user experience.
2. **Sharing marketing data with advertising platforms:**
   2.1. Rendin may send advertising data to platforms such as Meta Ads or Google Ads to enhance marketing notifications by using selected events (e.g., "registration: completed") and their attributes (e.g., system type, location, role). This data is used to optimize the User experience of the service and measure the effectiveness of advertising campaigns.
   2.2. The collected data is generally sent in a non-identifiable format. However, to optimize the relevance of advertisements, certain personal data may be sent in hashed (cryptographic hash functions) or anonymized form. This allows advertising platforms to link the data to an individual's profile without enabling direct identification. For anonymization, we use cryptographic hash functions.
   2.3. A limited set of personal identifiers, which the user has already shared on social media, is used to identify the User across different social media channels.
   2.4. Hashed personal data enables advertising platforms to analyze the impact of advertisements and identify suitable candidates within target audiences.
3. **Security and data protection**
   3.1. All transmitted data is protected using modern cryptographic methods to ensure data anonymity, making direct identification of the User impossible.
   3.2. Advertising platforms process data solely for the purpose of displaying Rendin advertisements and are prohibited from sharing data with third parties.
   3.3. Rendin does not share the methods for creating advertising target groups or other data sets with third parties.

## VI Cookies

Cookies are small text files placed on the user's device to collect standard internet logs and behavioral information. When visiting the Rendin platform, information may be collected through cookies or similar technology.

1. **Rendin utilizes two types of cookies:**
   1.1. Temporary or session cookies: These are deleted after the web browser is closed.
   1.2. Persistent cookies: These remain active after the browser is closed and can be used again when the User returns to Rendin's website.
2. **Purpose of cookies:**
   2.1. Rendin primarily uses first-party cookies to save User preferences, such as language selection and page settings. Cookies are also used to enable the use of the product platform anonymously before User registration and to later link the collected data to the registered account.
   2.2. Third-Party Cookies: Rendin uses third-party cookies in a limited scope (e.g., Meta and Google Ads) to monitor advertisement performance and optimize marketing activities.

3. **Objectives for using cookies:**
    3.1. Providing the service and ensuring the platform's functionality, including logging in, creating contracts, and other essential features. These cookies are essential for offering the service and are therefore mandatory.
    3.2. Improving the user experience, including analyzing platform usage to enhance services, make the platform more user-friendly, and provide a smoother user experience.
    3.3. Ensuring platform quality and monitoring, managing, and analyzing traffic. This helps identify technical issues and optimize website performance.
    3.4. Delivering relevant notifications and offers to users, which can help better understand or utilize the services.
    3.5. Protecting users and preventing fraud, by detecting and blocking suspicious activities and enabling a secure and reliable user experience.

Most cookies used are directly related to platform functionality and service provision, making them necessary for proper platform usage. These cookies cannot be disabled, as their absence would hinder the proper provision of services.

4. **Right to restrict data processing and modify consent:**
    4.1. Users have the right to modify their consent regarding the collection of cookies and marketing data at any time. It is also possible to opt out of sharing personal data with third-party advertising platforms by contacting us at info@rendin.co or by adjusting cookie settings directly in the web browser.

If a User wishes to limit or block cookies used by Rendin's service, they can do so by adjusting their web browser settings. For example, it is possible to block all cookies, accept only first-party cookies, or set cookies to be automatically deleted when the browser is closed.

It is important to note that not all Rendin services may function properly if all cookies are deleted or blocked.

**VII User Rights Regarding Personal Data Protection**

Users have the following rights regarding their personal data:

1. The User has the right to be informed of all data processing purposes before the processing takes place. If the User's consent is required for data processing, the User always has the option to refuse consent. Such consent is requested in the environment before the data is processed.
2. The User has the right to access their data.
3. The User has the right to data correction – the User may request Rendin to correct inaccurate data or complete incomplete data.
4. The User has the right to data deletion – under certain conditions, the User may request Rendin to delete their data (e.g., if the data processing is unlawful or if there is no legal basis for processing the data).
5. The User has the right to restrict and prohibit the processing of their data under certain conditions.
6. The User has the right to data portability – the User may request a machine-readable extract of the data collected by Rendin and have it transferred to themselves or another data controller.

If the User wishes to obtain information about the use of their personal data or exercise the aforementioned rights, Rendin requests that a digitally signed application be sent to the email address

info@rendin.co

**VIII Principles for processing personal data of other services**

The Rendin platform contains links to websites of other service providers. Our personal data processing principles apply only to the Rendin platform. If the User accesses links leading to third-party websites, we recommend reviewing the personal data processing principles and guidelines of the respective service provider on their websites.

**IX Changes to the privacy policy**

Rendin reserves the right to update its privacy policy in response to changes in data protection requirements, service development, adjustments to marketing activities, or other relevant reasons to ensure that privacy and data protection comply with current standards. Users will be informed of updates via the https://rendin.ee/legal page, and if necessary, we will also notify Users by email.

**X Contacting local regulators**

If the User wishes to file a complaint regarding the Rendin platform or service (including cases where the User feels that their concerns have not been adequately or sufficiently addressed), they have the right to contact the Consumer Protection and Technical Regulatory Authority (TTJA). TTJA's contact details are available at https://www.ttja.ee/

If the User believes that their rights regarding personal data processing have been violated, they may file a complaint with the Data Protection Inspectorate (AKI). AKI's contact details are available at https://www.aki.ee/