



Privacy Statement

1. Scope of Application and Acceptance

This privacy notice applies to all riskrate (hereinafter "riskrate") business processes and websites, domains, mobile solutions, cloud services, and third-party social networks.

This notice describes riskrate's data processing when riskrate is the data controller and data processing performed on behalf of customers following their instructions when riskrate is the data processor.

Personal data is information that can be used to identify a person, such as an address, email address, or phone number. We need to process your personal data in order to serve our customers. By providing us with your personal data, you accept the procedures and terms of this privacy policy.

2. Riskrate as Data Controller

Data security is important to us. Therefore, we collect and process data responsibly and with care for your privacy. This privacy statement describes how riskrate collects and uses your personal data when you use riskrate services and when you become a riskrate user.

Additionally, you will receive information about your rights and how you can exercise them.

1. Data Controller

Riskrate Oy Ab (3489461-2) www.riskrate.io

phone number: +358 50 367 0261 email: paivi@riskrate.io

2. Person Handling Registry Matters

Additional information about the personal data contained in the customer register, and their processing can be obtained from the data controller, either by phone, postal mail, or email (see contact details in section 1).

3. Name of the Register

Riskrate's customer register based on customer relationships and other legitimate connections of companies and company decision-makers/key persons ("Customer Register")

4. Purpose of the Register and Legal Basis

Customer Register: Personal data is processed for the implementation of services related to customer relationships and other legitimate connections, management and analysis of customer relationships, provision of services, business development and planning, marketing, distance selling, opinion and market research, and customer communication, which can also be implemented electronically and in a targeted manner.

Customer data may be processed for the following purposes:

- Initiating customer relationships and implementing software service
- Managing and developing customer relationships
- Verifying customer transactions, including payment transaction data
- Marketing, statistics, and analysis
- Other similar purposes related to customer relationship management

5. Data Content of the Register

The Customer Register may process the following information about all registered persons (to the extent existing/known):

- First name and last name
- Business ID
- Company name
- Phone number
- Email address
- Postal and/or visiting address
- Customer number
- Username and/or API key
- Start and end date and method of customer relationship and/or legitimate connection
- Direct marketing permissions and prohibitions
- Information about possible connections to other customers or organizations
- Customer offer and contract information (possible previous and current)
- Customer service order, usage, and payment transaction data
- Received customer feedback, including possible complaints

- Information regarding the use of electronic services and content (e.g., newsletter subscriptions)
- Information related to marketing and sales promotion, such as marketing activities targeted at the registered person and participation in them
- Received customer feedback, including possible complaints

In addition to the above, the Customer Register may process the following information about service purchasers:

- Billing information
- Contact persons (name, phone, email)
- Information related to managing customer relationships and other legitimate connections, communication, and classification (e.g., product and service purchase and cancellation information, delivery information, feedback, complaints, and recordings of customer service events such as calls, emails, and support messages)

Customer Register data may only be used for the purpose defined for it. However, data may be used in the data controller's other registers and for the data controller's own planning and statistical needs.

6. Regular Data Sources

Personal data concerning the registered person is collected from the registered person themselves, from various services used by the registered person (riskrate websites), and in connection with various marketing activities, such as phone contacts and marketing activities and marketing events, such as webinars, with the express consent of the registered person or their representative.

Personal data may also be collected and updated at the request of riskrate's customers or from their registers, as well as from authorities and companies providing personal data services.

Information about our customers is regularly obtained from:

- The customer themselves via websites, email, phone, during customer meetings, or in other similar ways
- Business information registers or other similar private or public registers
- The website of an existing or potential new customer or other public information sources published by them

In addition, information can only be obtained from elsewhere with the express consent of the registered person or their representative.

7. Regular Disclosure of Information

Information may be disclosed as required by requests from competent authorities or other parties, in accordance with applicable legislation.

Information may be disclosed to buyers in connection with corporate arrangements if riskrate sells or otherwise reorganizes its business.

8. Regular Disclosure of Information and Transfer of Data Outside the EU or European Economic Area

As a rule, data is not transferred outside the territory of the European Union member states or the European Economic Area, unless it is necessary for the purposes of personal data processing mentioned above or for the technical implementation of data processing, in which case the data transfer complies with the requirements of the data protection regulation.

9. Rights of the Registered Person

Right to Inspect and Correct

The registered person has the right to check the data stored in the register concerning them. Requests regarding the right to inspect must be made in writing and signed to the data controller's email address or postal address stated in this statement.

The data controller will provide a written response to the registered person within 30 days of the registered person's written inspection request being received by the data controller. If there are deficiencies or errors in the registered data, the registered person may submit a specified and justified request to correct the deficiency or error to the person responsible for customer register matters mentioned in this statement.

The data controller will delete, correct, or supplement incorrect, incomplete, or outdated information in the register on its own initiative or at the justified request of the registered person without undue delay.

The registered person has the right to prohibit the data controller from processing data concerning themselves for direct advertising, distance selling, and other direct marketing, as well as market and opinion research. For prohibition and correction matters, the registered person may contact the person responsible for the customer register mentioned in this statement.

10. Register Protection

Only those riskrate employees who have the right to process customer data by virtue of their work are authorized to use the electronic system containing customer data. All persons working with customer data are riskrate employees and have signed confidentiality agreements.

Each user has their own username and password to the system.

In addition, each user has been given data protection training, and an agreement regarding the confidentiality and secrecy of register data has been drawn up with them. Data is collected in databases that are protected by firewalls, passwords, and other technical means.

Manual Material

There is no manual material for electronically stored data. Personal data is protected from unauthorized access and illegal processing (e.g., destruction, alteration, or disclosure). Each processor can only process the personal data they need for their work tasks.

Automatically Processed Data

Electronically processed data contained in the register is protected by firewalls, passwords, and other technical means generally accepted in the information security industry.

11. Implementation of the Registered Person's Rights

The registered person has the right to check what data concerning them has been stored in the register.

At the registered person's request, we will make necessary corrections and additions to personal data or delete incorrect, unnecessary, incomplete, or outdated data from the perspective of the purpose of processing.

Data inspection and updating takes place by contacting the person responsible for riskrate's register matters at paivi@riskrate.io and +358 50 367 0261.

Riskrate retains your personal data only as long as it is needed for their stated purposes or to fulfill legal obligations. When the personal data we collect is no longer needed, we destroy or delete it securely.

12. Riskrate as Data Processor

Riskrate provides financial reporting services to its customers. These services involve processing customer data and possibly also processing personal data. Our customers determine the purpose of processing. In this case, the customer acts as the data controller.

Riskrate acts as the data processor and processes data according to the customer's instructions. When acting as a data processor, Riskrate complies with the data processing agreement made with the customer in accordance with the data protection regulation.

The customer has given their consent and guarantees that:

- The customer owns or is otherwise entitled to transfer the data to riskrate for processing and that the customer is responsible for the accuracy, correctness, content, reliability, and compliance with legal requirements of the data.
- The customer is obliged as the data controller to notify authorities and/or the data subject of a breach or unauthorized disclosure of personal data in the manner required by law.

When acting as a data processor, riskrate is obliged to take technical and organizational data security measures to protect privacy on behalf of the customer acting as the data controller.

As a data processor, riskrate does not process personal data in any way other than authorized in the agreement made with the data controller.

If data subjects have, for example, questions, comments, or requests concerning personal data processed by riskrate, they must be sent to the data controller. As a data processor, riskrate does not disclose personal data to data subjects unless the data controller has given instructions to do so. If the police or other authorities require the disclosure of personal data, riskrate will immediately notify the data controller and will only disclose the data by court order.

13. Automatic Data Collection

Riskrate uses commonly used digital marketing methods and tools to collect information about your movement in the service and on websites. This information is collected to improve the usability and content of the service and our websites, to target advertising

and marketing, and to determine the visitor's interests. Data collection mainly takes place through cookies (see below), and they cannot be linked to a person.

Cookies are small text files containing character strings that allow the browser to be uniquely identified. The website or a third party sends them to the computer. The use of cookies is regulated by laws such as Section 205 of the Information Society Code, according to which cookies, the storage of website usage data, and their purpose of use must be clearly and comprehensively communicated to the website user.

Most browsers are configured to accept cookies. However, you can change your browser settings so that the browser refuses to accept third-party cookies or notifies you of their transmission. You can get more information about cookies and how they work, for example, at www.allaboutcookies.org.

Cookies Used by Riskrate

We use cookies on our websites to better understand what content our website visitors are interested in.

Cookies also help us improve the user experience of the website. Analytics help us find errors on the website faster, such as broken links. The information can also be used to improve our advertising.

We do not identify the identity of visitors based on cookies on our websites, as we do not collect personal information with cookies, such as the user's name, address, or phone number. Our website also does not require registration.

For a new or existing customer, we collect information about login and its timing to the riskrate service through our homepage.

Information we collect with cookies:

- Time
- Duration of visit
- Pages used
- Browser type
- Whether the visitor has visited our website before
- Source of visitor traffic
- IP address

For Google tools used by Riskrate on its websites, you can prevent Google from collecting and processing data generated by Google cookies by downloading and installing the Google Analytics Opt-out Browser Add-on for your browser.

14. Changing the Privacy Statement

Riskrate continuously develops its business and therefore reserves the right to change this privacy statement. Changes may also be based on changes in legislation.

If we make changes to the privacy statement, we will update the modified notice in this privacy statement. We encourage you to read the notice regularly.

This privacy notice was last updated on May 13, 2026.

16. Contact

If you have comments or questions about our privacy statement, or if you are concerned about privacy protection or data use, or suspect that your privacy has been violated, send a message to paivi@riskrate.io. We will process your request confidentially and our representative will contact the address you provided if necessary. We will process any complaints without undue delay and as required.