Privacy policy

We care about our customers, which means we care about you and your privacy. We always collect personal information responsibly and with your privacy in mind. This privacy policy explains how riskrate collects and uses your personal information when you use riskrate Services, and when you become a riskrate User. In addition, you will know what rights you have and how to use them.

1. Register holder is BackedByCFO Oy Maria 01, Lapinlahdenkatu 16, 00180 Helsinki www.riskrate.io

2. Contact the person in charge of the Customer Register

For more information on the personal data included in the Customer Register and how to process it, please contact us, either by post (see address details in section 1) or by email to paivi@riskrate.io

3. Register name riskrate Customer Register

4. Purpose of the Customer Register

- Starting a Customer relationship and onboarding a software as a service
- Customer success management and PR
- Certification of Customer transactions, including payment management
- Marketing, statistics, and analytics
- Other uses for Customer success and relationship management

5. Content of the Customer Register

Customer Register contains the following information (to the extent that it exists / it's known)

- First name and last name
- Trade register or Business identification code
- Company name
- Telephone number
- email
- Address
- Customer code
- Customer user name and/or API key
- Connections to the other Customers or organizations
- Special offerings and agreements (not valid and valid agreements)
- Customer orders, transaction, and payment transactions
- Feedback and possible reclamations

riskrate may only the Customer Register information only for the intended use. However, the data may be used in the other registers of the Register holder, the business development, and for statistical purposes.

6. Regular data sources, information about our Customers are provided and collected regularly:

- From the Customer itself via web pages, by e-mail, telephone, customer meeting, or similar.
- Business registers or other similar private or public registers
- The website of an existing or potential new customer or publicly available information. In addition, information can only be obtained with the data subject's explicit consent.

7. Regular disclosure of information and data transfer outside the EU or the European Economic Area.

To the extent permitted by the Personal Data Act and the EU Data Protection Regulation, data may be transferred to and stored on behalf of a Register Holder outside the EU or the European Economic Area.

8. Rights of the data: Right of inspection and rectification

The data subject has the right to check the data stored in the register. Contact with the right of inspection shall be made in writing and signed to the postal address of the Register Holder specified in this Privacy Policy. The data subject shall submit a written reply to the data subject within 30 days of the receipt of the written check request from the data subject to the controller. If there are shortcomings or errors in the registered information, the data subject may, in this document, submit a request to the person responsible for the Customer Register for correction of the identified and justified defect or error. The Register Holder shall erase, correct or supplement, on its own initiative or following a reasoned request by the data subject, erroneous, incomplete or outdated information in the register without undue delay.

Prohibition of Right The data subject has the right to prohibit the Register Holder from processing data concerning him/her for direct marketing and other direct marketing and market and opinion surveys. In the case of prohibition and rectification, the data subject may be contacted by the person responsible for the customer register mentioned in this Privacy Policy.

9. Principles of Registry Security

- Manual data is not stored electronically.
- Only those employees who have the right to handle customer information for their work are eligible for the use of a customer information system.
- Each user has their username and password for the system.
- In addition, each user has been given training in data protection, and an agreement on the confidentiality and confidentiality of register information has

been drawn up with him. Data is collected in databases that are protected by firewalls, passwords, and other technical means.