

Privacy Notice

Updated: July 14, 2026

At SmartCap, we value your privacy. This Privacy Notice explains what we have done to ensure that your right to privacy is respected and protected.

Definitions

The General Data Protection Regulation (GDPR) means Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

Personal data means any information relating to an identified or identifiable natural person (for example, a name, personal identification code or email address).

Processing of personal data means any operation performed on personal data (for example, alteration, viewing, storage or erasure).

A cookie is a small text file that a website stores on a visitor's computer hard drive, smartphone or other device. Cookies send information to the website that may be used to recognise the visitor's device settings and preferences.

1. Whose personal data do we process and to whom does this Privacy Notice apply?

This Privacy Notice applies to you if you:

- apply for a job with us;
- work at SmartCap;
- visit our website;
- contact us;
- are associated with a company that participates as a tenderer in a public procurement procedure organised by us, or with a company that provides services to us;
- are associated with a company or fund in which we have invested, either directly or indirectly, or which has expressed an interest in receiving financing from us in the form of an investment.

Although the GDPR does not apply to legal persons, it does apply to natural persons associated with a legal person, such as its representatives, members of its governing bodies, shareholders, members, ultimate beneficial owners and others.

2. Who is responsible for processing your personal data?

The controller of your personal data is AS SmartCap (registry code 12071991).

You can contact us using the following details:

address: Sepise 7, 11415 Tallinn, Estonia

email: risks@smartcap.ee

3. What personal data do we process, for what purposes and on what legal bases?

SmartCap collects personal data to the extent necessary to achieve the business purposes described below. The personal data collected generally falls into one or more of the following categories:

- Identification data — first name and surname, date of birth, personal identification code, citizenship, permanent address, residency, identity document details (including a photograph of the document) and proof of residency;

- Contact details — address, telephone number and email address;
- Financial data — bank account details, account statements, payment details, income information, tax return information, payment defaults and information concerning the origin of assets;
- Professional data — job title, previous work experience, education, relevant licences and certificates, associated companies, holdings in legal persons, conflicts of interest, time commitment and motivation, information disclosed during interviews, information contained in a cover letter and solutions to practical assignments;
- Background and compliance data — information concerning previous offence proceedings, ongoing court proceedings, enforcement and bankruptcy proceedings, whether a person is subject to financial sanctions, links to sanctioned countries, political exposure and status, and the position held by a politically exposed person;
- Publicly available data — publicly available information (for example, a LinkedIn profile or data from the Commercial Register);
- Access and log data — access rights to IT systems and premises, and log data;
- Professional photograph — an employee's photograph published on the website only with the employee's consent;
- Website usage data — cookies and other data relating to visits to the website.

We collect and use personal data only for specific purposes. We generally process personal data for one or more of the following purposes:

- To assess potential direct and fund investments and to manage investments already made, we mainly use the identification, contact, professional and financial data of the ultimate beneficial owners, members of the management board, employees and other representatives of potential or actual portfolio companies. Depending on the circumstances, the legal basis for processing is taking steps prior to entering into a contract, performance of a contract, compliance with a legal obligation or legitimate interests.
- To carry out anti-money laundering and counter-terrorist financing checks, we use identification, contact, professional and other data to the extent necessary for such checks. The legal basis for processing is compliance with a legal obligation.
- To evaluate tenderers participating in public procurement procedures and to conduct such procedures, we mainly use the identification, contact and professional data of the tenderer's representatives and team members, including information submitted to demonstrate their qualifications. The legal basis for processing is compliance with a legal obligation and taking steps prior to entering into a contract.
- To perform any other contract entered into or to be entered into with you, we mainly use your identification and contact details and any other information whose processing is necessary for the performance of the relevant contract. The legal basis for processing is performance of a contract and taking steps prior to entering into a contract.
- When you apply for a job, we mainly use candidates' identification, contact and professional data and other information provided in application documents. The legal basis for processing is taking steps prior to entering into a contract.
- To conduct a background check, we use the selected candidate's identification data and other relevant information to the extent necessary to verify any current criminal convictions and prohibitions on engaging in business. The background check is conducted after a job offer has been made to the candidate and before the employment relationship begins. The legal basis for processing is your consent.
- To administer the employment relationship, we mainly use employees' identification, contact, financial and professional data and other information whose processing is necessary to fulfil obligations arising from the employment contract, including for payroll, leave, business travel, occupational health and further training. The legal basis for processing is performance of a contract and compliance with a legal obligation.
- To publish information about employees on SmartCap's website, we use employees' names, job titles and other information published with the employee's consent, including the employee's photograph. The legal basis for processing is the employee's consent.

- To handle whistleblowing reports, we use the data of the reporting person and the persons named in the report to the extent necessary to handle the report in accordance with the procedure established by law. The legal basis for processing is compliance with a legal obligation.
- To manage IT systems and premises, we use identification and contact details and information necessary to manage access to software, hardware, internal files and premises. The legal basis for processing is our legitimate interest in ensuring the organisation's information security and the security of its premises.
- To resolve disputes, we use the identification, contact and other data of the persons concerned to the extent necessary to resolve the dispute. The legal basis for processing is our legitimate interest in protecting SmartCap's rights and compliance with a legal obligation.
- When you visit our website, we process data collected through cookies.

SmartCap does not carry out automated individual decision-making or profiling.

4. Where have we obtained your data from?

We mainly collect data directly from you (for example, when you apply for a job with us, write to us or call us), but we may also collect data from persons associated with you (for example, from an investment target when making investments).

In certain cases, we may also collect data from external databases (for example, the Criminal Records Database, Creditinfo's payment default register and the Commercial Register when carrying out background checks).

Please note that the provision of certain data is required by law or contract. Failure to provide the required data may prevent us from establishing or continuing a business relationship or other contractual relationship with you.

5. Do we disclose your data and, if so, to whom?

We may share your data with independent controllers and processors where, for example, we are legally required to do so, where this is necessary to provide services to you or where it is necessary to protect our legitimate interests, including in connection with disputes.

Independent controllers include supervisory authorities (such as the Estonian Financial Supervisory Authority, the Estonian Data Protection Inspectorate and the Estonian Financial Intelligence Unit), the Ministry of Finance (the Public Procurement Register), legal service providers (various law firms), credit institutions (for the purpose of complying with requirements arising from anti-money laundering and counter-terrorist financing legislation), external auditors, courts, the Ministry of Economic Affairs and Communications (for the submission of data in the context of structural assistance) and our parent company, the Estonian Business and Innovation Agency. These organisations are independently responsible for processing your data as separate controllers.

We have also engaged service providers for certain activities, including in the fields of IT and telecommunications, who process your data on our behalf and under our responsibility as our processors. To support our work processes, we may also use cloud-based tools, including artificial intelligence solutions. Where personal data is processed through such tools, the processing takes place within the purposes and legal bases set out in this Privacy Notice, in approved environments and subject to appropriate safeguards. Outputs produced using automated tools are reviewed by a SmartCap employee before use.

We disclose your personal data only to service providers that have ensured the implementation of sufficient safeguards to protect the security of your personal data. Where necessary, we enter into data processing agreements with service providers setting out their obligations when handling your personal data.

Some third parties with whom we share your personal data may be located outside the European Union. In such cases, we ensure that at least one of the following safeguards is in place:

- The European Commission has determined that the country receiving the data ensures an adequate level of protection for personal data.
- The recipient is bound by contractual clauses approved by the European Commission that ensure a level of protection for personal data equivalent to that in the European Union. For further information, see the Standard Contractual Clauses for transfers of personal data between EU and non-EU countries. [Standard contractual clauses for data transfers between EU and non-EU countries are available here.](#)

6. Cookies

We use cookies on our website. Cookies are small text files stored on a visitor's device by the web browser when the visitor accesses the website. The cookies we use include strictly necessary cookies that are essential for the operation of the website.

7. How long do we retain your personal data?

SmartCap does not process personal data for longer than is necessary to fulfil the purposes described above, including to comply with statutory personal data retention obligations and to protect SmartCap's rights in ongoing or potential future disputes. Where processing is based on consent, we process personal data until consent is withdrawn, unless the law or accounting or reporting requirements require us to retain the data for longer.

Where the appropriate retention period for a category of personal data or individual data item is not clear, we determine an appropriate deletion period by taking into account the nature and scope of the data, the context and purposes of processing, and the potential harm to the data subject's rights and freedoms in the event of a personal data breach.

8. What are your rights and how can you exercise them?

You have the right to:

- obtain confirmation as to whether we process your personal data and, where we do, receive a copy of your personal data;
- withdraw your consent to the processing of personal data where we rely on your consent;
- request the rectification of your personal data;
- request the erasure of your personal data where we have no legal basis for processing it (for example, where the retention period has expired or there is no legal basis for its processing or further processing);
- request restriction of the processing of your personal data;
- object to the processing of your personal data where we rely on legitimate interests. In such a case, we are required to explain the legitimate interest on which the processing is based;
- request that your personal data be transmitted to a third party designated by you. This right applies only to data that you have provided to us and that we process electronically on the basis of your consent or a contract, provided that the transmission is technically feasible by reasonable means;
- lodge a complaint with the Estonian Data Protection Inspectorate (website: www.aki.ee).

To exercise your rights, please contact us using the contact details provided in Section 2. SmartCap will respond to your request without undue delay and no later than one month after receiving it. Where required due to the complexity or number of requests, SmartCap may extend the response period, provided that we inform you of the extension and the reasons for it no later than one month after receiving your request.

9. Data protection measures

SmartCap implements appropriate technical and organisational measures in accordance with the GDPR to protect your personal data against accidental or unlawful destruction, accidental loss, alteration, unauthorised disclosure or access, and any other unlawful processing.

Although SmartCap implements appropriate technical and organisational security measures to protect personal data, no method of data processing is completely secure. SmartCap therefore cannot guarantee the absolute security of personal data transmitted.

10. Application and amendment of this Privacy Notice

SmartCap may amend this Privacy Notice unilaterally at any time. The amended Privacy Notice will be made available on SmartCap's website. SmartCap will notify about the changes to this Privacy Notice on smartcap.ee and/or by other appropriate means within a reasonable period before the changes take effect, unless the changes result solely from amendments to legislation or do not affect the processing of the personal data of existing data subjects.

This Privacy Notice also applies to the processing of personal data relating to persons whose data we were already processing before this Privacy Notice entered into force.