# Privacy statement for the client register

Updated 6 March 2023

## 1. General

This privacy statement provides information to the controller's customer required by the EU General Data Protection Regulation and Finnish legislation.

## 2. Controller

Finnvera plc (Business ID: 1484332-4)
Street address: Porkkalankatu 1, 00180 Helsinki, Finland
Switchboard: +358 (0)29 460 11

## 3. Contact information

Contact: tietosuojavastaava@finnvera.fi

## 4. Register name

Finnvera's client register

## 4. What personal data we process

This privacy statement applies to persons related to Finnvera's corporate clients. The role may vary depending on whether the person is authorised to sign on behalf of the company or if they are an actual beneficiary, guarantor, pledger, owner of the company or its authorised representative.

Your personal data may be processed based on the type of connection you have to our corporate client. Processed data consists of:

- Identification details of persons acting on behalf of the company, such as name and personal identity code or other national personal identification, nationality and identity document, such as a copy of a passport, driving licence or other similar document.
- Contact details such as phone numbers, address details and e-mail address
- Information about your education, profession, work, competence and experience
-

## 5. Purpose of the processing of personal data

We process your personal data for the following purposes:

- offering products and services to our potential customers.

- customer service and client relationship management, including the management of the client's liabilities and receivables, the risk management and supervision of credit and guarantee operations, the payment of indemnification and the collection of receivables.

- fulfilment of requirements and obligations defined in law, regulations or decisions by supervisory or other authorities, including
    - the know-your-client (KYC) obligation pursuant to the regulations preventing money laundering and the financing of terrorism
    - sanctions-related checks

  - accounting regulations
  - reporting to police, debt recovery and supervisory authorities
  - obligations related to risk management (credit and securities risks) and capital adequacy requirements.

- Marketing services and our products and sending newsletters. We use cookies and similar technology on our website, including communications and marketing via social media platforms. More information on cookies is available in our cookie policies.

- Safety and security, Finnvera uses camera surveillance at the following offices: Lahti, Rovaniemi and Tampere. At our other offices, camera surveillance is by the owner managing the building.

- Developing our products and services to provide and develop even better service and customer experience.

**6. Legal basis for the processing of personal data**

According to Article 6 of the GDPR, there must be a legal basis for the processing of personal data. The legal basis is one of the following:

- You have concluded or intend to conclude an agreement with us (see Article 6 (1)(b) of the GDPR)
- Compliance with a legal obligation (see Article 6(1)(c) of the GDPR), for example:
  - Act on the State-Owned Specialised Financing Company 18 June 1998/443
  - Act on Credits, Guarantees and Capital Investments Provided by the State-Owned Specialised Financing Company 18 June 1998/445
  - Act on the State's Export Credit Guarantees 23 May 2001/422
  - Act on Preventing Money Laundering and Terrorist Financing (444/2017)
  - Act on the Customer Data System for Enterprise Services (293/2017)
- A legitimate interest (see Article 6(1)(f) of the GDPR), the controller's legitimate interest is based on a customer relationship or similar relationship between Finnvera and the data subject. The controller ensures that such processing of data is proportionate to the data subject's interests and meets their reasonable expectations.
  - For example, direct marketing or product and service development

Processing tasks may be outsourced to the controller's external service providers in accordance with the data protection legislation and within the framework laid out by legislation.

**7. Storage period of personal data**

We store your data for as long as necessary for the purpose of their collection and processing or for as long as required by law and regulations.

We store your data necessary for the customer relationship for at least the duration of the customer relationship. After the termination of the customer relationship, the storage period depends on the data in question and its purpose. We fulfil legal data storage obligations. For example:

Agreement data is deleted approximately ten years after the end of an agreement. Customer relationship information, such as KYC information, is deleted or anonymised approximately ten years after the last agreement ends.

We aim at ensuring that the personal data we process is accurate and up to date by erasing unnecessary data and updating obsolete data. However, we recommend that you check your information from time to time.

## 8. Regular sources of data

We primarily collect personal data directly from you. In addition, personal data may be collected and updated, to the extent permitted by law, from third-party registers, such as:

- Registers maintained by authorities (e.g. the Population Register Centre, the Tax Administration's registers, business registers, enforcement authorities, the police)
- Credit information controllers
- Information need for determining political power and inclusion within the scope of the international sanctions adhered to by the controller from parties that maintain such databases

## 9. Regular disclosure of data and groups of recipients

Pursuant to the Act on the Customer Data System for Enterprise Services (293/2017), data can be disclosed to the organisations referred to in the Act. The register can be used to store and process information related to public enterprises. Information that can be stored in the register includes:

- Identification details: name, home country, domicile, street address, e-mail address and telephone number as well as the person's title and role in the company
- Information on entrepreneurial advice or other service received by a person and identification details of the person to whom the service has been provided
- Changes to the above information

Data related to voluntary and judicial collection of receivables is transferred once a day as line transfer to the external service provider Intrum Oy. Disclosed data consists of:

- information about the parties – basic information
- basic financing information
- invoice
- financing payment scheme

## 10. Transfer of data outside the EU or the EEA

No regular transfer of data to countries outside the EU or the European Economic Area.

We use subcontractors and partners to produce and provide services, which is why your personal data may be transferred to such parties for processing on our behalf. These parties will only be able to process your data in accordance with our instructions and they will not have access to your data for their own purposes, such as direct marketing.

We will ensure through contractual and other arrangements that our subcontractors and partners always process your data carefully and in accordance with good data processing practices.

As a rule, we process your data within the EEA. The EEA includes the EU Member States as well as Iceland, Liechtenstein and Norway. If we transfer data outside the EEA to a country whose national regulations do not guarantee EU-level data protection, we will ensure an adequate level of protection of personal data as required by law and use the

data transfer mechanisms approved by the European Commission, primarily the standard contractual clauses of the European Commission.

The standard contractual clauses are available on the website of the European Commission:

Standard contractual clauses for international transfers | European Commission (europa.eu)

**11. Principles of register protection**

Your personal data is only processed by those Finnvera employees whose work duties require them to process the data. The access rights of the register are restricted with personal user IDs and passwords.

The controller's personnel are committed to complying with confidentiality obligations. In addition, the employees have committed to complying with internal information security guidelines.

Manual materials are stored in locked and guarded facilities.

We use appropriate technical and organisational safeguards to protect your personal data. Such means include proactive and reactive risk management, various protection and filtration techniques as well as access control and safety systems. Safeguards also include security planning, controlled granting and monitoring of access rights, ensuring the competence of personnel involved in the processing of personal data, and careful selection of subcontractors. We update our internal practices and guidelines continuously.

Pursuant to Section 6 of the Act on the Customer Data System for Enterprise Services (293/2017), the Ministry of Economic Affairs and Employment, acting as the technical administrator of the system, is responsible the integrity, protection and storage of the data in the system.

The purpose of the aforementioned measures is to secure the confidentiality of the personal data stored in the register, the availability and integrity of data as well as the realisation of the rights of the data subjects.

**12. Automated decision-making**

Finnvera does not make decisions based on automated decision-making. Finnvera also does not conduct profiling based on the personal data it processes.

**13. Your rights**

You have the legal right to access data, the right to rectify data, the right to request the erasure of data i.e. "right to be forgotten", the right to restriction of processing, the right to object to processing, and the right to have data transferred from one system to another (data portability).

**Right of access**

If you want to check your data, you have to submit an access request with the Messages function in the e-services under Other. (You can log in to the e-service with your personal banking IDs or a mobile ID).

**Right to rectification**

If your personal data in our possession is inaccurate or incomplete, you have the right to request the rectification of such data, unless this right is restricted by law.

**Right to erasure**

You have the right to the erasure of data in certain cases, but due to legislation, we have a statutory obligation to store your personal data for the entire duration of the customer relationship and even after it has ended.

**Right to object to the processing of personal data**

If you find that the data we have stored about you is incorrect or if you have objected to the use of the data, you may request that the use of your personal data be restricted so that we only have the right to retain your data until the accuracy of the data can be verified or until it can be verified whether our legitimate interests override your interests.

If you have the right to have your personal data in our possession deleted, you can ask us to restrict the processing of the data to its retention instead of deleting it. If we only need the data to defend a legal claim, you can also request that other use of the data be limited to its retention. However, we may have the right to use the data for other purposes, such as defending a legal claim, or in the case that you have given your consent for using the data for other purposes.

**Right to withdraw consent**

You have the right to withdraw your consent at any time without it affecting the legality of the processing carried out before the withdrawal of consent if the processing is based on your consent or express consent.

**Complaint to the supervisory authority**

You have the right to file a complaint or contact the Office of the Data Protection Ombudsman. The contact information is available on the Office’s website.

**14. Contact information**

In all matters concerning the processing of personal data and the exercise of your rights, you can contact the Finnvera Data Protection Officer at tietosuojavastaava@finnvera.fi.

If you want to check your data, you have to submit an access request with the Messages function in the e-services under Other. (You can log in to the e-service with your personal banking IDs or a mobile ID).