PRINCIPLES FOR PROCESSING CLIENT DATA

(Valid from 31 July 2025)

I. Introduction

By setting up a personal account on ESTO's Website and/or requesting ESTO Services, the Client confirms that they have thoroughly reviewed the principles of client data processing described in this document.

ESTO's principles for processing client data explain how ESTO collects, uses, and protects Clients' Personal Data.

ESTO presents information on the processing of client data herein as follows: first, the Client is provided with a quick overview of the key points and clicking on a specific topic will bring up a more detailed description of that topic. The principles for processing client data provide information on the following issues:

- How are the terms used in the principles for processing client data defined and what general provisions apply?
- Who is the Controller for Clients' Personal Data?
- What categories of Personal Data does ESTO collect and process about its clients, and from what sources are Clients' Personal Data collected?
- For what purposes and on what legal basis does ESTO process Clients' Personal Data?
- Does ESTO use automated decision making or profiling to process Personal Data?
- To whom does ESTO transfer Personal Data and for what purposes?
- Does ESTO transfer Personal Data outside the European Economic Area?
- How long does ESTO retain Personal Data?
- What rights does the Client have in relation to the processing of their Personal Data?
- How can ESTO change these Principles?
- Where can Client ask questions related to the processing of Personal Data or if they wish to exercise any of their rights related to the processing of Personal Data?

II. Definitions

2.1. **ESTO** – the creditor providing financial services, ESTO AS (registry code 14180709, address Laeva 2, Tallinn, Estonia, 10111).
2.2. **Client** – a natural person who visits ESTO's Website, has expressed their desire to create an account on ESTO's website and/or wishes to apply for ESTO's services, or uses or has used ESTO's services.
2.3. **Personal Data** – any information relating to an identified or identifiable natural person ("data subject").
2.4. **Client Data** – any information (including Personal Data) that ESTO has about the Client.
2.5. **Processing** – any operation or set of operations performed on personal data or on sets thereof, whether or not by automated means, such as collection, structuring, use, transmission, querying, extraction, modification, erasure, etc.
2.6. **Client Relationship** – the legal relationship between ESTO and the Client that arises when the Client uses or has used ESTO's Service or has contacted ESTO for the purpose of using the Service.
2.7. **Third Party** – any natural or legal person other than the Client, ESTO, the Processor or persons who may process Client Data while acting under the direct supervision of ESTO or the

Processor.

2.8. **Contract** – the contract between ESTO and the Client under which ESTO provides the Service to the Client.

2.9. **Principles** – these principles for processing client data.

2.10. **Controller** – a legal person who, alone or jointly with others, determines the purposes and means of the processing of personal data. ESTO is considered the Controller of the Client's Client Data.

2.11. **Processor** – the person who processes Client Data on behalf of ESTO.

2.12. **Service** – payment and financial services provided by ESTO to the Client. An overview of the services offered by ESTO can be found on ESTO's Website.

2.13. **Website** – ESTO' website at www.esto.eu, through which the Client can access the ESTO self service environment.

2.14. **General Data Protection Regulation** or **GDPR** – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

III. General Principles and Controller details

3.1. ESTO Processes Client Data in accordance with the requirements of the General Data Protection Regulation, the Personal Data Protection Act, other relevant legislation and these Principles. The terms and conditions for Processing Client Data may also be described in documents related to ESTO's Service and in Contracts entered into with Clients. Where these Principles contradict the terms and conditions of documents related to ESTO's Service or of any Contract concluded with the Client regarding the processing of Client Data, the terms and conditions provided by the documents related to the Service or in the Contract shall prevail.

3.2. As a licensed Estonian financial services provider, ESTO is considered the Controller in the Processing of Client Data for the purposes of the General Data Protection Regulation. If you have any questions regarding the Processing of Client Data or wish to submit a request related to the Processing of Personal Data, please contact us by using the contact details provided in section XII of these Principles.

3.3. ESTO and its employees are required to keep Client Data confidential and are liable for any breach of their obligations. Only employees who have received appropriate training are permitted to access and process Client Data. Client Data are Processed only to the extent necessary for the performance of the assigned tasks and the fulfilment of obligations arising from legislation.

IV. Types and sources of Client Data to be processed

4.1. ESTO processes the following personal data about the Client:

Identifying data	Given names and surname, personal identification code, date of birth, address, place of birth, identity document details, data on the country of residence and citizenship.
Authentication and security data	Authentication method used to log in to the user account on the Website (e.g. ID card, Mobile ID, Smart ID, SMS code), authentication history (date/time, IP, location), information related to security incidents (e.g. attempt to log in to the account with an incorrect password).
Contact details	Phone number, address, e-mail address, language of communication.
Financial data	Client's income (salary or other income), liabilities, assets (including information on the origin of assets), previous payment history, account transactions, contracts entered into and terminated, applications submitted, statements submitted, interest and service fees,

	breaches of contract.
Data on client's professional activities	Data about the Client's professional activities, including the Client's level of education.
Data concerning private life	Number of dependents, information on whether the Client is a politically exposed person.
Data on offences	Information on economic and professional offences, offences against property, etc, which involve or may involve the use of financial services (e.g. money laundering, terrorist financing, violation of sanctions), court judgments in relation to offences, together with the reasons for the judgments, and offences that are the subject of ongoing proceedings.
Information on the Client's reliability	Information about previous payment behaviour and fulfilment of assumed commitments, credit rating, information about possible links to money laundering or terrorist financing, data on offences, judicial dispositions, media coverage, the publication *Ametlikud Teadaanded*.
Information on external sanctions and PEP lists	Sanctions lists and lists of persons considered to be politically exposed persons (PEPs) contain information such as name, date of birth, place of birth, function or position, and the reason why the person has been included in the list.
Information on use of ESTO's services	What services has the Client used (including data on previous and current contracts)? This includes information about existing and past debts, arrears, as well as your payment and repayment history.
Purchase data	Information about the goods or services the Client wishes to purchase using ESTO's services and information about the merchant from whom the Client wishes to purchase the goods/services.
Client service information	Communications sent by the Client to ESTO, including requests, complaints, recordings of telephone conversations (if the Client decides to contact ESTO by phone); data obtained through other means of remote communication.
Newsletter data	Information on whether the Client wishes to receive newsletters and notifications about special offers to their contact details.
Website usage data	Data about visits to the Website; data related to visits to the self-service environment, including data about when and where the user logged in; system and technical records about the Client's activities; Client settings; the IP (Internet Protocol) address used by the browser, the website from which the Client accessed ESTO's Website; the device used.
Information obtained in the course of performing legal obligations	Information resulting from inquiries/claims sent by courts, investigative bodies, tax authorities, enforcement agents, notaries.

4.2. ESTO collects Client Data from the following sources:

4.2.1. The majority of Client Data are provided to ESTO by the Client themselves when

they create an account on the Website, submit a request for the Service or enter into a Contract with ESTO;

4.2.2. The service provider to whom ESTO has delegated certain activities in accordance with the law. The above person acts as an independent Controller in the processing of Clients' Personal Data, and the service provider processes the Client's Personal Data in accordance with the rules established by it.

4.2.3. The merchant from whom the Client has made a purchase while expressing their wish to use ESTO's Service to pay for the purchase;

4.2.4. Public databases and private registers (e.g. the publication *Ametlikud Teadaanded*, the pension register, Internet search engines, the population register, the register maintained by Krediidiinfo, the commercial register);

4.2.5. Information about the Client's connections With Third Parties (e.g., whether the Client is a politically exposed person);

4.2.6. From a company within the ESTO group.

V. Purpose and legal basis of processing

5.1. ESTO provides a summary table below describing the methods of collecting Client Data, the purposes of processing Client Data, the legal bases for processing Client Data, and matters relating to the retention of Client Data.

5.1.1. The purposes of processing Client Data in connection with the creation of a personal account on the Website

Purpose of processing	Personal data processed in order to accomplish the purpose	Legal basis for processing personal data	Retention period for Personal Data
To identify the Client, create a personal account for the Client, and enable secure login to the Client Account	- Identifying data - Contact details	**Client's consent** (Article 6(1)(a) of GDPR) as long as the Client has not submitted a request for the Service.	Pending withdrawal of consent
		To perform a contract or take steps prior to entering into a contract (Article 6(1)(b) of GDPR), if the Client has applied for the Service through their account and enters into a Contract with ESTO. **To comply with the obligations provided by the Money Laundering and Terrorist Financing Prevention Act** (Article 6(1)(c) of GDPR).	Retained for 5 years from the end of the business relationship.
To detect fraud	- Identifying data - Authentication and security data	**ESTO's legitimate interest in preventing, detecting, and investigating potential fraud or misuse that may harm ESTO, its clients, or its partners** (Article 6(1)(f) of GDPR).	Retained for 1 year from the date of collection (unless the Client has submitted a request for the Service or entered into a Contract)
Client Relationship management in accordance with the Contract entered into between ESTO and the Client for each Service used. This includes compiling and providing information to the Client in electronic form (not	- Identifying data - Authentication and security data - Contact details - Service used by the Client	**To perform a contractor to take steps prior to entering into a contract** (Article 6(1)(b) of GDPR)	Retained for 5 years from the end of the business relationship

for marketing purposes)			
To assist the Client in using the account	- Identifying data - Authentication and security data - Contact details - Client service information - Website usage data	**ESTO's legitimate interest in providing the best customer service** (Art. 6(1)(f) of GDPR)	Retained for 5 years from the end of the business relationship
To send marketing information to the Client regarding offers, products or services provided by ESTO's partners.	- Contact details - Newsletter data	**Client consent** (Article 6(1)(a) of GDPR)	Pending withdrawal of consent
to conduct client satisfaction surveys, organise consumer research and request feedback from Clients via e-mail, text messages, telephone or other communication channels.	- Contact details - Information on use of ESTO's services	**ESTO's legitimate interest to improve its Services** (Art. 6(1)(f) of GDPR)	Until the end of the business relationship
5.1.2. Purposes for processing Client Data in connection with requesting the Service and to enable use of the Service.			
To prevent money laundering and terrorist financing and to ensure compliance with international sanctions (e.g. applying due diligence measures when establishing and monitoring business relationships)	- Identifying data - Contact details - Financial data - Data on client's professional activities - Data concerning private life - Information on the Client's reliability	**To comply with the obligations provided by the Money Laundering and Terrorist Financing Prevention Act** (Article 6(1)(c) of GDPR).	Retained for 5 years from the end of the business relationship

	- Information on external sanctions and PEP lists - Information on use of ESTO's services - Data on offences - Purchase data		
To assess the suitability of the Client for the Service requested by the Client	- Identifying data - Contact details - Financial data - Data on client's professional activities - Data concerning private life - Information on the Client's reliability - Information on external sanctions and PEP lists - Information on use of ESTO's services - Data on offences - Purchase data	**Implementation of the principle of responsible lending as provided by § 403[4] of the Law of Obligations Act** (Article 6 (1(c) of GDPR).	Personal Data are retained for 3 years after the end of the business relationship
To assess the creditworthiness of the Client and manage credit risk	- Financial data - Data concerning private life - Data on client's professional activities - Information on the Client's reliability - Information on use of ESTO's services	**To comply with the obligations provided by the law** (Article 6(1)(c) of GDPR).	Retained for 3 years from the end of the business relationship
Automated decision-making and profiling for creditworthiness assessment	- Financial data - Data on client's professional activities - Purchase data - Information on reliability - Use of client services	**ESTO's legitimate interest** (Art. 6(1)(f)	Retained for 5 years from the end of the business relationship
To detect fraud	- Identifying data - Authentication and security data - Information on use of ESTO's services	**ESTO's legitimate interest in preventing, detecting, and investigating potential fraud or misuse that may harm ESTO, its clients, or its partners** (Article 6(1)(f) of GDPR).	Retained for 5 years from the end of the business relationship

To improve the quality of ESTO's Services, develop systems, and compile statistics	- Website usage data - Client service information - Information on use of ESTO's services	**ESTO's legitimate interest in improving its Services** (Article 6(1)(f) of GDPR)**.**	Retained for 5 years from the end of the business relationship
Ensuring security, logging systems and preventing intrusions	- Website usage data - Authentication and security data	**ESTO's legitimate interest in preventing, detecting, and investigating potential fraud or misuse that may harm ESTO, its clients, or its partners** (Article 6(1)(f) of GDPR).	Retained for 5 years from the end of the business relationship
To profile the client and provide them with personalised Services	- Contact details - Newsletter data - Financial data - Information on use of ESTO's services	**Client consent** (Article 6(1)(a) of GDPR)	Retained until consent is withdrawn.
To respond to inquiries from authorities, including courts, enforcement agents, trustees in bankruptcy, tax officials, investigative authorities, and the Financial Intelligence Unit	- Information obtained in the course of performing legal obligations - Identifying data - Contact details - Financial data - Data concerning private life - Information on use of ESTO's services	**To comply with the obligations provided by the law** (Article 6(1)(c) of GDPR).	Retained for 5 years from the end of the business relationship
5.1.3. When contacting ESTO's customer service			
To assist the Client in applying for or using the Service	- Identifying data - Information on use of ESTO's services - Contact details	**ESTO's legitimate interest in ensuring the best customer experience** (Article 6(1)(f) of the GDPR)**.**	Retained for 5 years from the end of the business relationship

VI. Automated decisions and profiling

6.1. ESTO uses both Client profiling and automated decision-making in the provision of the Service to make sure the Service is provided effectively.

6.2. **Profiling** is any form of automated processing of Personal Data intended to evaluate personal aspects relating to a natural person, such as profiling carried out to evaluate the economic situation, personal preferences, interests, reliability, or location of a Client.

6.3. ESTO uses profiling for the following purposes:

6.3.1. To prevent fraud and other abuses and mitigate risks;
6.3.2. To assess the risks in complying with anti-money laundering and terrorist financing requirements;
6.3.3. To assess the likelihood of insolvency;
6.3.4. To provide a personalised Service, including customising content and recommendations.

6.4. **An automated decision** is a decision made entirely without the intervention of an ESTO employee and which has a significant impact on the rights or opportunities of the client. The automation of certain decisions helps to speed up the decision-making process and make it more impartial and transparent.

6.5. ESTO uses automated decisions based on Client profiling to achieve the following objectives:

6.5.1. assess the Client's financial situation and the likelihood of insolvency;
6.5.2. identify potential fraud or money laundering risks.

6.6. When making automated decisions, the Client's user behaviour and financial situation are checked against typical risk behaviours and conditions. These different factors are combined through an automatic decision-making model into an aggregate result (score), which is used to decide whether or not to grant the Service request and what the terms and conditions of the Service are for the Client.

6.7. ESTO makes automated decisions when it:

6.7.1. Decides to offer the Service to the Client under ESTO's terms and conditions;
6.7.2. Decides not to provide the Client with ESTO's Services;
6.7.3. Decides that the Client's actions indicate a risk of fraud;
6.7.4. Decides that the Client's conduct may indicate money laundering or that the Client is on sanctions lists.

6.8. If the automated decision made by ESTO about the Client is negative, the Client cannot use ESTO's Service. To ensure the legitimacy and relevance of its decisions, ESTO has implemented several safeguards, including regular model reviews and random checks.

6.9. Automated decisions and profiling are based on Personal Data known about the Client, which has been collected in accordance with these Principles. Such processing of Personal Data is carried out in accordance with ESTO's legitimate interest.

6.10. The Client has the right to receive explanations about automated decisions and profiling, to express their views and to contest the decision. To this end, a corresponding request must be submitted using ESTO's contact details provided in section XII of these Principles.

VII. Transmission of Client Data

7.1. ESTO may transfer the Client's Personal Data to third parties, who may be either independent Controllers or Processors authorised by ESTO.

7.2.ESTO transfers Clients' Personal Data to the following third parties:

Public authorities (e.g. supervisory authorities, courts, enforcement agents, police, the prosecutor's office)	where the obligation to transfer Personal Data arises from the law or where ESTO has a legitimate interest in protecting itself against crimes.
Maintainers of databases and registers (e.g., population register, commercial register, payment default register, and other registers, the Tax and Customs Board, Pensionikeskus)	for the purposes of implementing the responsible lending principle and verifying the information provided by the client when making a credit decision
Companies belonging to the same group as ESTO	in order to provide the Service to the Client, improve the quality of the Service, and comply with statutory obligations
ESTO's advisers (e.g. auditors, legal advisers)	where necessary for the performance of an audit or for legal advice
Providers of financial services	where necessary for the provision of the Service or offering a financing solution to the Client
Companies offering identity verification	to ascertain the identity of the Client, verify the accuracy of the data and prevent fraud and criminal activity
Merchants from whom the Client wishes to purchase goods or services.	for the purposes of transaction execution and customer service
Companies performing creditworthiness assessments (e.g. Taust.ee, CreditInfo)	where the Client has submitted a request for a Service that requires ESTO to assess the Client's solvency, ESTO will make an inquiry about the Client to obtain information about the Client's credit score and any potential debts
Payment service providers	for the purpose of processing payments and carrying out transactions
Service providers	to whom ESTO has delegated its activities in accordance with the law, provided that they comply with data protection requirements and confidentiality obligations
Providers of IT services needed to provide the service (e.g. server, network and communication services, analytics services, communication service provider, call recording)	to enable the operation of the platform, data processing, sending automatic and manual e-mails/SMS messages to Clients, recording conversations with Clients
Marketing service providers	for running ads, campaigns and managing client interaction
Debt collection companies	where the Client has not met their payment obligations under the contract, to ensure debt collection
Recipients and intermediaries of debt claims (e.g. investment platforms)	to the extent that ESTO has reassigned its claims against the Client arising from the Contract

VIII. Transfer of Client Data outside the European Economic Area

8.1. As a rule, ESTO does not transfer the Client's Personal Data outside the European Economic Area. However, if ESTO's Processors or Third Parties end up having to do this, the background of the Processor or Third Party will be thoroughly checked beforehand, and appropriate safeguards will be put in place for data transfers and protecting Client Data.

8.2. If Client Data are transferred outside the European Economic Area, appropriate safeguards are implemented, e.g. transfer of data to a country for which the European Commission has adopted a decision on the adequacy of the level of data protection or transfer of data on the basis of standard data protection clauses drafted by the European Commission.

8.3. Pursuant to Article 49(1) of the General Data Protection Regulation, personal data may be transferred outside the European Economic Area in the absence of safeguards where, for example, it is necessary for the performance of a contract between the Client and ESTO or for the implementation of pre-contractual measures taken at the Client's request or for the conclusion/performance of a contract between the Client and another person or for the establishment, exercise or defence of legal claims.

IX. Retention of Client Data

9.1. ESTO shall retain Client Data in a personalised form for as long as it is necessary for the purposes of processing personal data and/or for performing obligations arising from legislation.

9.2. ESTO follows these key retention periods when storing Client Data:

9.2.1. If ESTO processes the Client's personal data based on their consent, this is done until the Client withdraws their consent;

9.2.2. ESTO retains personal data collected in the performance of obligations provided by the Money Laundering and Terrorist Financing Prevention Act for 5 years after the expiry of the business relationship (subsections 1 and 3 of § 47 of the Money Laundering and Terrorist Financing Prevention Act).

9.2.3. ESTO retains personal data collected in the performance of obligations provided by the Creditors and Credit Intermediaries Act for 3 years after the expiry of the contract entered into with the Client (subsection 5 of § 47 of the Creditors and Credit Intermediaries Act).

9.2.4. ESTO retains personal data collected in the performance of its obligations under the Accounting Act for 7 years (subsection 1 of § 12 of the Accounting Act).

X. Client's rights

10.1. The Client has the following rights:

10.1.1. **Right of access** – the Client has the right to know what data ESTO has collected about them, for what purpose they are being processed; to whom data are disclosed; from whom data are obtained (other than the Client); how long data are stored; what are the Client's rights regarding the correction, erasure and restriction of processing of data.

10.1.2. **Right to rectification** – the Client has the right to request the correction of Personal Data concerning them where such data are incorrect or incomplete.

10.1.3. **Right to erasure** – in certain cases, the Client has the right to request that ESTO erase their Personal Data, for example if the Client has withdrawn their consent for ESTO to process their data and there is no other legal basis for further processing, or if ESTO has processed personal data unlawfully.

10.1.4. **Right to restriction of processing** – in certain cases, the Client has the right to prohibit or restrict the processing of their Personal Data for a certain period (e.g. if the

Client has objected to the processing of data).

10.1.5. **Right to object** – The Client has the right to object to the processing of Personal Data based on ESTO's legitimate interest, including profiling carried out on such legal basis. Upon submission of an objection, we are required to terminate processing, unless ESTO can demonstrate that the Client's Personal Data are being processed for compelling legitimate grounds that override the interests and rights of the data subject, or if the processing is necessary for the establishment, exercise or defence of legal claims.

10.1.6. **Right to data portability** – if the processing of Personal Data is based on the Client's consent or on a contract with ESTO and data are processed automatically, the Client has the right to receive the Personal Data concerning them that they have submitted to ESTO in a structured, commonly used and machine-readable format. The Client also has the right to request ESTO to transfer data directly to another service provider, if technically possible.

10.1.7. **Right to withdraw consent to the processing of Personal Data** – if the legal basis for processing Personal Data is the Client's consent (e.g., for sending direct marketing messages), the Client may withdraw their consent at any time. If the Client withdraws their consent, ESTO will no longer process their data for the purposes described in the consent form. Withdrawal of consent has no effect on the lawfulness of data processing based on the consent before its withdrawal.

10.1.8. **Right to lodge a complaint** – the right to lodge a complaint with the Estonian Data Protection Inspectorate or a court upon violation of their rights. However, ESTO recommends that you first contact ESTO so that we can clarify and resolve the situation as quickly and efficiently as possible.

10.2. In order to exercise their rights as a data subject, the Client may contact ESTO using the contact details provided in these regulations. ESTO will respond to any queries within 1 month of receiving them.

XI. Amendment and application of principles

11.1. ESTO reserves the right to unilaterally amend these Principles from time to time. Upon amending the Principles, ESTO shall notify the Client of its intention to amend the Principles via the Website at least one (1) month prior to the amendments taking effect, unless the amendments are based solely on amendments to legislation. Where the new terms and conditions refer to the processing of Your personal data for a new purpose that requires Your prior consent, we will not process Your personal data for such new purpose until we have obtained Your consent to this end.

11.2. The latest version of ESTO's regulations on the processing of personal data is always available on ESTO's website at www.esto.eu/ee.

11.3. The Principles for Processing Client Data have been drafted in Estonian and translated into English and Russian. In the event of disputes, the Estonian version of the Principles for Processing Client Data shall be legally binding.

XII. Contact details

12.1. If the Client wishes to receive additional information about the processing of their Personal Data, submit complaints related to the processing of Personal Data, or exercise their rights related to the processing of Personal Data, the Client can contact ESTO using the contact details below.

ESTO's contact details	ESTO's data protection specialist's contact details

ESTO AS Laeva 2, Tallinn 10111, Estonia info@esto.ee	**ESTO AS** Laeva 2, Tallinn 10111, Estonia info@esto.ee Please include the keyword "Data protection Specialist" in your letter or e-mail.