Valid as of 5 February 2022

OP-Public
5.2.2024

Privacy Notice

1 General Information

This Privacy Notice contains information on the principles of processing of personal data required by 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 (hereinafter the General Data Protection Regulation) and data protection legislation in the Republic of Estonia, that is, for customers, their representatives, security providers of OP Corporate Bank plc Estonia branch and for the supervisory authority.

2 Controller and its contact information

OP Corporate Bank plc Estonia branch
Address: Maakri 19/1, 10145 Tallinn
E-mail: info@opbank.ee
telephone +372 663 0840

3 Data Protection Officer's contact information

OP Corporate Bank Estonian branch Data Protection Officer, Silver Liisma
Address: Maakri 19/1, Tallinn
E-mail: silver.liisma@opbank.ee
Telephone: +372 663 0840

If you are a NetBank user, you can also send us a message via NetBank.

4 Personal data file

The data subjects of the data file are the controller's customers and potential customers (self-employed persons), representatives, owners, beneficial owners of corporate and institutional customers (hereinafter the company), security providers and potential security providers. The term "customer" used in this Privacy Notice includes all of the mentioned roles.

5 Purposes of personal data processing and legal basis for processing

5.1 Purposes of use of personal data

In this customer data file, personal data is used primarily to produce, offer, deliver and develop the controller's services, such as account and financing services. Below you can find more detailed information on how personal data is used in the data file:

- customer service and customer relationship management and development
- provision, development and quality assurance of services
- business development
- fulfilling statutory obligations and any other official rules and regulations
- risk management
- ensuring the security of services and investigating abuses

Automated decision-making and profiling

OP Corporate Bank plc Estonia branch does not use profiling and automated decision-making. All our decisions are made by a specially designated decision making body.

Preventing crimes

Know Your Customer (KYC) information and other data subject's personal data may be used to prevent, uncover and detect money laundering and terrorism financing as well as for other purposes required by the Law on the Prevention of Money Laundering and Terrorism Financing. The data subject's personal data may be used to investigate whether the person is subject to international sanctions followed by the controller.

The controller may process personal data concerning crimes or suspected crimes made directly against the operations of the credit institution if that is necessary in order to prevent and detect such crimes.

5.2 Legal bases of processing

Personal data is processed in the data file based on several legal grounds, the application of which is described with illustrative examples below.

1 Contractual relationship or actions preceding the conclusion of a contract, such as
   - Establishing a customer account
   - Personal data processing necessary for contract enforcement

2 Statutory obligation, such as
   - Industry-specific legislation, such as the Credit Institution Law
   - Other statutory personal data processing, such as cooperation with the police or tax authorities, and obligations related to reporting to the authorities

3 Performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, such as
- Law on the Prevention of Money Laundering and Terrorism Financing

4 Legitimate interests
- Data disclosure within OP Financial Group may be based on a legitimate interest
- Protection of the controller's interests at the law enforcement institutions, including establishment, exercise or defence of legal claims may be based on a legitimate interest.

In most cases, the controller's legitimate interests are based on the customer relationship or similar relationship between the controller and the customer. The controller also ensures that such processing is proportionate to the data subject's benefits and meets his/her reasonable expectations.

6 Categories of personal data

Data subjects are typically subject to processing the categories of personal data and personal data described below. The data content to be processed depends, for example, on whether it is the question of the data of a private individual (self-employed person) or of a person acting on behalf of the company.

Category of personal data	Example of content of data
Basic information	data subject's name, personal ID., postal address, phone No., email address, person's position in a company
"Know Your Customer" (KYC) information	statutory KYC information such as the information required to identify the customer and to determine their financial status and political influence
Contract and product information	the controller's and data subject's contract information; Information on products and services acquired by the data subject
Recordings and content of messages	recordings and messages in various formats, in which the data subject is a party, for example, video footage, phone call recordings.

7 Recipients and recipient groups of personal data

Any personal data obtained may be used within OP Financial Group as permitted by the law. In addition, personal data my be disclosed, for example, to:

- relevant authorities, such as the Estonian Financial Supervision and Resolution Authority, the Bank of Estonia, Estonian Tax and Customs Board;
- the European Central Bank, other central banks in the European System of Central Banks, European Investment Bank,
- vendors operating as the controller's partners.
- Creditinfo payment default register

8 Transfer of personal data

The controller uses suppliers in data processing, and data will be transferred outside of the EU or EEA to a limited extent. When data is transferred outside of the EU or EEA, the transfer is done using the EU Commission's standard contractual clauses or some other transfer mechanism in accordance with legislation.

Some of the controller's suppliers are other OP Financial Group entities or partner companies. They provide the controller with information system and other support services, among other things.

9 Personal data retention period or criteria for determining the period

Personal data may be processed during the validity of the customer and contractual relationship. It will also be processed after the end of the customer and contractual relationship for a period deemed necessary at any given time and what is stated below. Personal data is kept for up to 10 years after the termination of the contract for the protection of legitimate interests in the event of a civil law claim.

For example, we retain your KYC information for a minimum of 5 years up to 10 years after the end of the customer relationship. In case the establishment of relationship was rejected we retain the data for 12 months since the application date. We comply with statutory obligations in retaining data. The information will be erased in accordance with the controller's erasure processes.

The controller may be obligated to process some personal data in the data file for a longer period than stated above to comply with legislation or requirements set by the relevant authorities, such as capital adequacy measurement regulation.

10 Personal data sources and updates

Personal data is primarily collected from the data subjects themselves or, on a case-by case basis, from the entity on whose behalf they act. Within the limits permitted by the law, personal data may also be obtained from other OP Financial Group entities for risk management purposes.

Personal data can also be collected and updated within the limits permitted by law from the personal data files of third parties, examples including:

- Register maintained by Estonian Transport Administration (Traffic register)
- Registers maintained by Estonian Information System Authority (Commercial Register, Criminal Records Database)
- Registers maintained by the Estonian Ministry of Interior (Population registry)
- Registers maintained by AS Creditinfo
- Parties that maintain databases with information that is necessary to identify politically exposed persons and parties subject to international sanctions followed by the controller.

11 Data subject's rights

Data subjects have the right to receive confirmation from the controller as to whether their personal data will be processed or not.

If the controller processes a data subject's personal data, the data subject has the right to receive the information on the personal data being processed.

The data subject also has the right to request the controller to rectify or erase their personal data.

In certain cases, the data subject will also have the right to request the controller to restrict the processing of their personal data or to otherwise oppose the processing. In addition, under the General Data Protection Regulation, the data subject may request that the data they have provided themselves be transferred in machine-readable format.

All of the above requests must be submitted to the above-mentioned contact person of the controller. Before accepting the data subject's request the controller will identify the data subject. For the purpose of identification of the data subject, digitally signed request/queries can be submitted by sending an email to OP Corporate Bank Estonian branch Data Protection Officer.

If a data subject considers that his/her personal data is not processed legally, he/she has the right to file a complaint with the Estonian Data Protection Inspectorate. To contact Data Protection Inspectorate, visit www.aki.ee/en.

12 Protection methods regarding the data file

The controller processes personal data securely and in a manner fulfilling the requirements of applicable laws. It has carefully assessed the risks that may be associated with the processing and taken the necessary measures to manage these risks.

The controller has protected the data appropriately in technical and organisational terms. The data file is protected using, for example, the following tools:

- Protection of equipment and files

- Access control and access rights

- User identity verification

- Registration of usage events

- Processing guidelines and supervision

The controller also requires of its suppliers the appropriate protection of personal data to be processed.