

This document specifies the client data processing principles of AS TBB Bank Group (hereinafter the Bank). The Bank processes client data in accordance with the stipulated Principles. The Principles are applied, if the Client uses, has used or has requested to use the Bank's services or products or is otherwise connected to services and products. The Principles are also applied to the Client relationships created before the enforcement of the Principles.

1. Definitions

Client is a natural person or a legal person who uses, has used or has requested to use the products or services provided by the Bank or who is otherwise connected to products and services provided by the Bank.

Client data is any information (incl information handled as the banking secret and personal data) known by the Bank regarding a Client or its representatives.

Personal data is any information directly or indirectly related to the Client as a natural person.

Processing is any procedure performed with Client data (incl collection, recording, retention, changing, providing access, making inquiries and forwarding of data etc).

AS TBB pank is a public limited company established in Estonia.

AS TBB panga Grupp is AS TBB pank and its subsidiaries (AS TBB liising, AS TBB Invest, Morgan Trade AS).

Processor is a person processing Client data upon the request of the Bank.

Principles are the client data processing principles stipulated in this document.

2. General provisions

2.1. These Principles specify the general principles of client data processing by the Bank. The additional terms of client data processing could be also specified in the contracts, other documents related to services and products and on the Bank's website www.tbb.ee.

2.2. The Bank ensures the confidentiality of client data within the applicable law and applies appropriate technical and organizational measures to protect client data against unauthorized access, illegal processing or disclosure, accidental loss, changes or destruction.

2.3. The Bank is a controller of Client data.

2.4. The Bank can use processors for Client data processing. In such cases the Bank ensures that the processors process Client data according to the Bank's guidelines and in accordance with applicable law and apply proper security measures.

2.5. The regulations applicable to the cookies by the Bank are available on the Bank's website www.tbb.ee

3. Collection of Client data

The Bank collects Client data:

- from the Client;
- in using services and products by the Client;
- from external sources, such as public and private law registries (incl from the Tax and Customs Board

based on the agreement of the Client, Population Register etc);

- other third persons

4. Client data categories

The client data categories mainly, but not only, collected and processed by the Bank, are the following:

4.1. **Identification data**, e.g. name, personal identification code, date of birth, data on the identity document (e.g. copy of passport or ID card).

4.2. **Contact data**, e.g. address, phone number, e-mail address, language of communication.

4.3. **Family data**, e.g. data on the dependants and heirs of the Client

4.4. **Data on the Client relations with legal persons**, e.g. data submitted by the Client or obtained from the public registers or through third persons for making transactions in the name of the above legal person.

4.5. **Professional data**, e.g. data on the education or professional career.

4.6. **Financial data**, e.g. accounts, assets, transactions (incl security transactions), credits, income, obligations, incl payment data – declared income (excl income from transfer); salary and other payments of employers (based on TSD); incapacity benefits, unemployment insurance payments and redundancy payments, pensions, payments to the third pension tier, funded pension payments (based on TSD); entries made to the employment register (information on the employer and employment relationship); dividends and payments made from owners' equity, tax arrears from 100 euros.

4.7. **Payment data**, e.g. name of the payer and receiver, amount of payment, payment specification, account number, personal identification code, address, data of card transactions.

4.8. **Data on the origin of assets or income**, e.g. data on the transaction partners and business activities of the Client.

4.9. **Data on reliability and due diligence**, e.g. data on the payment performance; damage caused to the Bank or third person; data enabling the Bank to fulfil its due diligence measures related to money laundering and terrorist financing prevention and ensure the compliance with international sanctions, including the aim of business relationship and whether the Client is a politically exposed person.

4.10. **Data obtained and/or created in the course of fulfilment of the obligation resulting from law**, e.g. data proceeding from the inquiries made by investigative bodies, notaries, tax authority, courts and bailiffs, data on income, credit liabilities, real estate management, notations, historical notations and debts.

4.11. **Data on the Client's tax residency**, e.g. data on the country of residence, tax identification number and citizenship.

4.12. **Communication data**, e.g. visual and/or audio recordings collected when the Client visits the Bank's office or communicates with the Bank by phone or other data collected through e-mail, messages and other communication mechanisms, e.g. social media, data related to visiting the Bank's website by the Client or

- communication through other Bank's channels (e.g. internet and mobile bank).
- 4.13. **Data related to services and products**, e.g. fulfilment or non-fulfilment of contracts (incl insurance contracts), performed transactions, concluded and terminated contracts, submitted applications, inquiries and complaints, interests and service fees.
- 4.14. **Data on the habits, preferences and satisfaction**, e.g. activity of using services and products, used services, personal devices, answers to the questionnaires, lifestyle, hobbies, Client's satisfaction.
- 4.15. **Data related to participation in campaigns**, e.g. prizes won in campaigns.
- 5. Objectives and bases for client data processing**
The Bank processes Client data mainly:
- 5.1. **To manage client relationships and enable access to products and services:**
Objective: to conclude the contract with the Client and its fulfilment (e.g. for making the transfer), to keep the data updated and correct by checking and completing the data through external and internal sources.
Legal basis of processing: fulfilment of the contract or application of measures prior to the conclusion of the contract upon the request of the Client or the fulfilment of the legal obligation.
- 5.2. **To conduct creditworthiness and risk assessments:**
Objective: to conduct internal creditworthiness and risk assessments to specify the services and products to be provided to the Client and what are the terms; to manage the Client's debts; to ensure compliance with applicable law related to the creditworthiness and risk assessments in providing credit or other financial services, in risk hedging; related to the Bank's capital requirements; at the internal calculations and analyses.
Legal basis of processing: fulfilment of the contract or application of measures prior to the conclusion of a contract as requested by the Client, Client's agreement (single agreement for data inquiry from the Tax and Customs Board) or fulfilment of the legal obligation or at the Bank's legitimate interest for reliable risk management.
- 5.3. **To protect the interests of the Client and/or Bank:**
Objective: to protect interests of the Client and/or Bank and examine the quality of products and services provided by the Bank and to certify the business transactions or other business communication (recorded through conversations).
Legal basis of processing: fulfilment of the contract or application of measures prior to the conclusion of a contract as requested by the Client or fulfilment of the legal obligation or Client's agreement or Bank's legitimate interest.
Objective: to ensure safety of the Bank and/or the Client, protect the life and health of the Client and its representatives and other rights of the Bank and the Client (through visual and/or audio recordings).
- Legal basis of processing: The Bank's legitimate interest to protect its Clients, employees, visitors and their and Bank's assets.
- 5.4. **To provide additional services, conduct client satisfaction surveys, market analyses and do statistics:**
Objective: to provide services of the Bank or cooperation partners, including personal offers.
Legal basis of processing: Client's agreement or Bank's legitimate interest to provide additional services.
Objective: to conduct Client's surveys, market analyses and do statistics, organize campaigns for the Client.
Legal basis of processing: Bank's legitimate interest to improve Bank's products and services, improve user experience of services for the Client and develop new products and services upon legitimate interest of the Bank or/and agreement of the Client.
- 5.5. **To fulfil legal obligations and establish identity:**
Objective: to comply with applicable law and international contracts, for example related to responsible lending, application of principles of "fulfilment of due diligence regarding the Client" and "know your Client"; disclose the details of transactions related to performed investments to meet the market transparency requirements and notify the competent authorities of the latter, prevent, discover, examine and inform about potential money laundering and terrorist financing, if financial sanctions have been established for the Client or the latter is a politically exposed person, and establish identity.
Legal basis of processing: fulfilment of the contract or application of measures prior to the conclusion of a contract as requested by the Client or at the fulfilment of the legal obligation or at Bank's legitimate interest for reliable risk management and general management.
- 5.6. **To avoid misuse of products and services and ensure conformity and quality of products and services:**
Objective: to enable and control access to digital channels and monitor their functioning, avoid unauthorized access to digital channels and their misuse and ensure the information security.
Legal basis of processing: application of necessary measures prior to the conclusion of the contract; fulfilment of the contract; fulfilment of the legal obligation or Client's agreement or Bank's legitimate interests to ensure control on the authorities, access and operations of the Bank's digital services.
Objective: to enhance technical systems, information technology structure, adapt the view of service to the equipment and develop the Bank's services through testing and improvement.
Legal basis of processing: Bank's legitimate interest.
- 5.7. **To certify, perform and protect legal requirements, incl waive claims and give over the contracts.**
Legal basis of processing: fulfilment of the contract or application of measures prior to the conclusion of a contract as requested by the Client or fulfilment of the legal obligation or Bank's legitimate interest for execution of legal claims.

5.8. To perform transactions through payment system

Objective: to fulfil the obligations to conduct international transactions through credit institutions and national payments through national, European and international payment systems and comply with the rules and obligations provided, inter alia, in the European and international standards and certification systems related to card and security.

Legal basis of processing: fulfilment of the contract or application of measures prior to the conclusion of a contract as requested by the Client or fulfilment of the legal obligation.

6. Profile analysis, making personal offers and automated decisions

6.1. Objective: The profile analysis is an automated processing of personal data used for the assessment of specific personal qualities of the Client, for instance to analyse or estimate the economic situation, personal preferences, interests and residence of the person. The profile analysis can be used in advising the Client, for marketing purpose and in making automated decisions e.g. for assessment of creditworthiness, risk management, insurance risk assessment and control of transactions in fighting fraud.

Legal basis of processing: The legitimate interest of the Bank or fulfilment of the legal obligation or contract or agreement of the Client. The profile analysis is also used for the purpose of money laundering prevention based on the fulfilment of legal obligation.

6.2. Objective: The Bank can process Client data to improve user experience of digital services, e.g. adaptation of service views to the used device and creating of personal offers to the Client. The potential marketing options could be based on the service types used by the Client and navigation in digital channels.

Legal basis of processing: The legitimate interest of the Bank or fulfilment of the legal obligation or contract or agreement of the Client.

6.3. Objective: The Bank can also collect statistical data on the Client, e.g. typical code of conduct and way of life based on demographic household data. Statistical data for creating segments/profiles can be collected from external sources and these can be combined with the Bank's internal data.

Legal basis of processing: The legitimate interest of the Bank or fulfilment of the legal obligation or contract or agreement of the Client.

7. Client data processing and forwarding to third persons pursuant to law

7.1. The Bank has the right to process and forward Client data without Client's agreement to third persons on the bases resulting from law and namely:

7.1.1. to fulfil the tasks resulting from the legal acts to the Bank of Estonia and Financial Supervision Authority;

7.1.2. to the court or to the person mentioned in the court ruling in the cases set by law;

7.1.3. to the pre-trial investigation institution and prosecutor's office in started criminal procedure, also pursuant to the

procedure stipulated in the international agreement based on the application of legal aid arrived from the foreign country;

7.1.4. to the bailiff according to the code of enforcement procedure, to the bankruptcy trustee in cases stipulated in the Bankruptcy Act, also to the security authority for the fulfilment of the tasks stipulated in the Security Authorities Act;

7.1.5. to the tax authority according to the provisions of the Taxation Act and Tax Information Exchange Act, also based on the regulation substantiated in the started misdemeanour procedure;

7.1.6. to the State Audit Office for the fulfilment of its tasks;

7.1.7. to person entitled to inherit or the person authorized by the latter, also to the notary and to the person having made the inventory of the estate appointed by the notary and estate administrator appointed by court, also to the foreign consular representations in submitting the relevant written documents as to the estate and the related data;

7.1.8. to the person appointed by the Guarantee Fund based on the Guarantee Fund Act;

7.1.9. to the foreign financial supervision authority or other financial supervision authority through the Financial Supervision Authority, if the bank secrecy obligation expands to this authority;

7.1.10. to the executor of control over the declaration of interests to control the correctness of the data submitted in the declaration based on the Anti-corruption Act;

7.1.11. to the Tax and Customs Board as to the data required for the conduct of state supervision stipulated in the Gambling Act, also in case and within scope stipulated in the Income Tax Act;

7.1.12. personal data stipulated in the Tax Information Exchange Act to the Tax and Customs Board;

7.1.13. to the registrar of credit register (incl to Creditinfo Eesti AS) provided the Client has non-fulfilled financial obligation in the Bank. The Client data to be processed in the register of Creditinfo Eesti AS and their processing terms can be seen on the website www.krediidiinfo.ee;

7.1.14. to the financial institution belonging to the same consolidation group with the Bank and other credit institution which requires data on the history of fulfilment of payment obligations of the Client for the calculation of capital requirements of credit risk and application of responsible lending principles;

7.1.15. to the investigator, prosecutor and court related to the Bank's violated or disputed decision or freedom protection pursuant to the procedure set by law;

7.1.16. to the Financial Intelligence Unit and Security Police Board in the cases and within scope set in the Money Laundering and Terrorist Financing Prevention Act and International Sanctions Act.

8. Client data processing and forwarding to the third person for the conclusion and fulfilment of the contract

8.1. By entering to the transaction relationships with the Bank or by expressing will to enter into the transaction relationships with the Bank, the Client gives an agreement

to process personal data and forward to the third persons and namely:

- 8.1.1. to the banks involved in making national express payments and international bank transactions, correspondent banks, payment intermediaries, other financial institutions, e.g. Society for Worldwide Interbank Financial Telecommunication;
- 8.1.2. to the payment service providers, payment intermediaries, international card organizations, insurers, e-invoice issuers, sureties, guarantors, Estonian Central Register of Securities, notaries and other third persons related to the fulfilment of the contract;
- 8.1.3. manager of national databases (land, commercial, population register) related to the need to control the correctness of personal data;
- 8.1.4. to the legal persons belonging to the same consolidation group with the Bank with the aim to identify the Client, clarify the origin of the Client's assets, assess its solvency, provide appropriate financial service to the Client, conduct of marketing campaigns, waive the right of Bank's claim (non-fulfilled financial obligation of the Client) etc;
- 8.1.5. to the internal and external auditors of the Bank and legal persons belonging to the Bank's consolidation group;
- 8.1.6. to the professional legal persons providing collection services to waive the right of claim (non-fulfilled financial obligation of the Client) of the Bank or the legal person belonging to the same consolidation group with the Bank.
- 8.1.7. within the frame of cooperation contracts concluded for the provision of bank service to the Bank's cooperation partners (e.g. support contracts of licence agreements etc);
- 8.1.8. to the person providing services to the Bank (auditor, provider of legal assistance service etc).

9. Geographical district of processing

- 9.1. In general the Client data are processed within the European Union/European Economic Area (EU/EEA), but in some cases these are forwarded and processed in the countries that are located outside EU/EEA.
- 9.2. The client data are forwarded and processed outside EU/EEA provided there is a legal basis, e.g. fulfilment of legal obligation or Client's agreement and appropriate protective measures are applied. Appropriate protection measures are for example the following:
 - there is a valid contract including the standard contract terms created by EU or approved codes of conduct, certifications and other similar that corresponds to the General Data Protection Regulation;
 - the country located outside EU/EEA where the receiver is situated has the adequate data protection level according to the decision of the European Commission;
 - the receiver has been certified based on the data protection framework Privacy Shield;
 - (applied to the receivers located in the United States of America).

In case of address the Client receives more detailed information on the forwarding of Client data to the countries located outside EU/EEA.

10. Data retention periods

- 10.1. Client data are not processed longer than is necessary. The retention period could be based on the contracts with the Client, legitimate interest of the Bank or applicable law (e.g. acts related to accounting, anti-money laundering acts or the acts related to expiry term, other private law).
- 10.2. At the termination of the contract concluded with the Client to continue to process the Client data, if this is required for the fulfilment of the obligation set in the legal acts, also for the purpose to ensure the data retention to settle the disputes arising from the contracts concluded with the Client.
- 10.3. Pursuant to the termination of the contract concluded with the Client the Bank continues the processing of Client data, if this is required to fulfil the obligation set in the legal act or retain the data to settle the dispute arising from the contract concluded with the Client.

The Bank retains the Client data in general for up to 10 years after the termination of the relation with the Client, i.e. if the contracts concluded with the Client have expired, if no direct obligation to retain the Client data within other term is arising from the legal act.

11. Rights of the Client as the private person

- 11.1. The Client as the private person has the following rights related to the processing of personal data:
 - 11.1.1. to apply for the correction of the personal data, if these are inadequate, deficient or incorrect;
 - 11.1.2. to submit objections regarding the processing of its personal data, if the use of personal data is based on the legitimate interest, including on the profile analysis for the purpose of direct marketing (e.g. receipt of marketing offers or participation in questionnaires);
 - 11.1.3. to apply for the cancellation of its personal data, e.g. if the personal data are processed at its consent or if it has withdrawn its consent. Such right is not applied, if the personal data asked to be cancelled are additionally processed also on other legal bases, e.g. on the basis of the contract or for the fulfilment of the legal obligations;
 - 11.1.4. to restrict the processing of its personal data based on the applicable law, e.g. during the period the Bank assesses whether the Client has the right to cancel its data;
 - 11.1.5. to obtain information on whether the Bank processes its personal data and if it processes, to obtain the overview on the abovementioned data;
 - 11.1.6. to obtain its personal data submitted by itself and that are processed based on the consent or for the fulfilment of the contract in writing or in general electronic format and, if technically possible, to forward these data to other service provider (data portability);
 - 11.1.7. to withdraw its consent for the processing of its personal data;

- 11.1.8. to request that no decision is adopted as to it that is based only on the automated decision, including profile analysis, if this involves the related legal consequences or has considerable impact on it. This right is not applied, if the decision making is required for the conclusion or fulfilment of the contract with the Client, if the decision making is allowed based on applicable law or the Client has provided its explicit consent.
- 11.1.9. To file complaints on the use of personal data to the Estonian Data Protection Inspectorate (website: www.aki.ee), if it finds that its personal data processing infringes its rights and interests pursuant to applicable law.
- 11.2. The restriction of the rights of the Client by the Credit Institution in processing the personal data of the private person:
- 11.2.1. If the Bank processes the Client's personal data:
- at the conduct of monitoring of business relationship for the purpose of money laundering and terrorist financing prevention;
 - for the purpose of tax frauds and market abuse prevention;
 - for the purpose of meeting the security requirements and application of risk management measures.
- 11.2.2. If the Bank processes the Client's personal data for the purpose of ensuring the operations of payment services.
- 11.3. The rights of the Client are restricted by adjusting the following terms: different types of personal data are not processed; the Bank documents all reasons in implementation of fulfilment of security requirements and application of risk management measures; the Bank applies appropriate measures to protect the rights and freedoms of the Client; the Bank applies all suitable and appropriate security measures stipulated in article 32 of Regulation (EU) 2016/679 of the European Parliament and Council and does not retain data in the personified format longer than is required for the achievement of objectives, incl for following the retention obligation arising from law, unless the deletion of the data endangers the operations of tax system and the Bank applies suitable and appropriate measures which ensure that the data are not processed for any other purpose than for the fulfilment of the objectives stipulated by law.
- 12. Contact information**
- 12.1. The Clients can contact the Bank related to the inquiries and cancellation of agreements and the Clients as the private persons can additionally require the exercising of its rights in processing the personal data and submit the complaints on the use of personal data.
- 12.2. The Bank's contact information has been provided on the website of AS TBB pank: www.tbb.ee
- 12.3. The contact information of the appointed data protection specialist for the Client as the private person: Vana-Viru 7, Tallinn, e-mail: andmekaitse@tbb.ee, marked as "Data protection specialist".
- 13. Validity and changes of the Principles**
- 13.1. The Principles are available for the Clients in the Bank's offices and on the website www.tbb.ee.
- 13.2. The Bank has the right to change this procedure unilaterally, by notifying the Client of this two months in advance pursuant to the procedure stipulated with the Bank's General Terms.
- 13.3. In any unregulated matters the Bank proceeds from the Credit Institutions Act, Personal Data Protection Act, General Data Protection Regulation of the European Union, guidelines of the Financial Supervision Authority and other legal acts.
- The present version of the Client data processing Principles of the Tallinn Business Bank has been approved by the Management Board of Tallinn Business Bank on 18 December 2019.**