AS "PNB Banka", reg. No. 40003072918
15-2 Elizabetes street, Riga, Latvia, LV-1010
Phone: (+371) 67041100, fax: (+371) 67041111
e-mail: info@pnbbanka.eu, www.pnbbanka.eu

# PERSONAL DATA PROCESSING REGULATIONS

## Table of Contents



## 1. Terms and Abbreviations Used

1.1. **Bank** – AS **"**PNB Banka**"**.

1.2. **BRD** – Bank's regulatory documents (including procedures, regulations, instructions).

1.3. **Commission** – a permanent Data Protection Commission established by the Bank by the decision of the Management Board of the Bank, which operates in accordance with the Bank's **"**Regulation on the Data Protection Commission**"**.

1.4. **Data** – any information relating to an identified or identifiable Data Subject in accordance with the requirements of the Regulation.

1.5. **Data Processing Impact Assessment** – an assessment performed by the Bank on the impact of planned processing of Data on Data protection, the results of which are summarised in the Form **"**Data Protection Impact Assessment**"** approved by the Bank.

1.6. **Data Subject** – a Bank's client (a natural person who plans to enter or has entered into an agreement with the Bank on the receipt of financial or other services), Bank client's legal representative, beneficial owner or another third party who is directly or indirectly related to the client and whose Data are processed by the Bank within the framework of fulfilment of its functions, as well as a natural person who is a representative, beneficial owner of a Bank's client or potential client/legal person, or another third party who is directly or indirectly related to the Bank's client.

1.7. **Officer** – a person designated by the Bank who fulfils the duties of a data protection officer under a contract within the framework of the tasks set by the Regulation and who complies with the criteria set in Article 37(5) of the Regulation.

1.8. **Processing of Data** – any operations which are performed by the Bank on the Data or on sets of Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.9. **Protection of Data** – a set of technical and organisational measures applied by the Bank to ensure the protection of Data, including Special Categories of Data, and the security of processing of Data.

1.10. **Regulation** – 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 (General Data Protection Regulation).

1.11. **Responsible Employee** – an official of the Bank or an employee of the Bank's structural unit who performs the processing of Data of the Data Subject within the framework of his or her competence.

1.12. **Special Categories of Data** – data which comply with the criteria set in Article 9(1) and Article 10 of the Regulation.

1.13. **Supervisory Authority** – the Data State Inspectorate, i.e., an authority which supervises the compliance of processing of personal data to the requirements of the Regulation within the framework of the competence determined in the Personal Data Processing Law of the Republic of Latvia.

1.14. The terms stipulated in this Clause are hereinafter used with capital and small initial letters, as well as in singular and plural.

## 2. General Regulations

2.1. These Regulations lay down the principles relating to the processing of Data observed by all the officials of the Bank and employees of Bank's structural units.

2.2. The Bank shall apply the conditions of these Regulations also in legal relations which the Bank has established with service providers, if they provide financial and other services on behalf of the Bank or ensure the processing of Data by order of the Bank.

2.3. Bank's officials, structural units and their employees shall, in implementing the conditions of these Regulations, observe the general principles relating to the lawful processing of Data and Data protection determined in the Bank's "Privacy Policy", as well as the recommendations of the Officer and the Commission regarding the correct, lawful and fair processing of Data.

2.4. The regulatory framework included in these Regulations shall have no retroactive effect and its operation shall apply solely to legal aspects which occur following the entry into force of these Regulations.

2.5. The Bank shall ensure that activities relating to the processing of Data shall be carried out by all officials of the Bank and employees of Bank's structural units, who have become acquainted with BRD in the field of Data processing and

protection, as well as have signed the Form “Deed of Commitment on Non-disclosure of Business Secret and Official Secret” approved by the Bank.

2.6. The Bank shall revise these Regulations at least once a year.

## 3. Officer and Commission

3.1. **Creation of the Officer’s Position, Officer’s Status, Rights and Duties.**

3.1.1. The Bank shall create the Officer’s position, as the Bank, in implementing its functions, performs the processing of Data, including Special Categories of Data, which is regular, systematic and large scale by virtue of their nature, scope and purpose.

3.1.2. The Bank shall ensure that the Officer is directly subordinate to the responsible Member of the Bank’s Management Board.

3.1.3. The Bank shall ensure that the Officer is duly and timely involved in all matters concerning Data protection.

3.1.4. The Bank shall support the Officer, ensuring the following:

1) the resources necessary to perform tasks determined in these Regulations and other BRD;
2) access to the Data and the processing of Data by the Bank;
3) the possibility of improving knowledge in the field of Data protection.

3.1.5. In order to ensure the observance of requirements for the prevention of a conflict of interests, the Bank shall:

1) ensure that the Officer receives no instructions with regard to the performance of the tasks determined in these Regulations and other BRD;
2) not dismiss the Officer or not apply sanctions to the Officer, except cases where there are justified reasons which are not related to the performance of the tasks set by the Regulation for the Officer;
3) ensure that none of the tasks and duties assigned by the Bank results in a conflict of interests, if the Bank has assigned the Officer to perform other tasks and duties which are not related to the performance of the tasks set by the Regulation.

3.1.6. The Officer shall have the following duties:

1) to organise, control and monitor the compliance of processing of Data by the Bank with the requirements of the Regulation, the laws and regulations of the Republic of Latvia in the field of data protection, and the Bank’s “Privacy Policy”;
2) to inform and consult the Members of the Bank’s Management Board and Bank’s employees about their duties in accordance with the Regulation, the laws and regulations of the Republic of Latvia in the field of data protection, and the Bank’s “Privacy Policy”;
3) to consult the Data Subject on matters relating to the processing of his or her Data and the exercising of rights provided for by the Regulation, the laws and regulations of the Republic of Latvia in the field of data protection, and the Bank’s “Privacy Policy”, if such request has been received;
4) to maintain registers which include information on activities relating to the processing of Data to the extent determined in Article 30 of the Regulation and which are submitted to the Supervisory Authority at the request thereof;
5) at request, to provide advices with regard to the Data Processing Impact Assessment and monitor the implementation thereof;
6) to cooperate with the Supervisory Authority, as well as within the activities determined by BRD — with other authorities, organisations and subjects of private law;
7) to be the contact person of the Supervisory Authority in matters relating to the processing of Data, including preliminary discussion, if the Data Processing Impact Assessment indicatively shows that planned activities relating to the processing of Data are likely to result in a high risk, and to provide consultations in the relevant case;
8) to assess and harmonise draft BRD and other draft documents prepared by the Bank, if the content of the relevant documents is related to the processing or protection of Data;
9) to conduct training for Bank’s employees on matters concerning the processing and protection of Data;
10) to fulfil the duties of the Chairperson or Member of the Commission in accordance with the conditions of the Bank’s “Regulation on the Data Protection Commission”;
11) to organise and implement an audit of the Data processing and Data protection system;
12) to observe the secrecy and confidentiality provisions set by the Bank.

3.1.7. In order to implement the duties determined in Clause 3.1.6 of these Regulations, the Officer shall have the following rights:

1) to carry out inspections in the structural units of the Bank, to examine and become acquainted with the Bank’s operations, processes, resources and documents, to ask questions, to request for explanations, to receive replies and the copies of necessary documents from any Bank’s employee;
2) to propose the development of BRD or BRD amendments on the processing of Data and protection of Data;
3) to consider and provide recommendations on BRD and BRD amendments prepared by other structural units of the Bank, which affect or can affect the lawfulness of processing of Data by the Bank or the protection of Data;
4) to participate in the work of the Bank’s committees, commissions and work groups with the rights of an adviser, if matters relating the lawfulness of processing of Data or the protection of Data are examined;
5) to prepare mandatory tasks relating to the processing of Data or the protection of Data, setting deadlines and designating responsible employees of the Bank (determination of tasks is harmonised with the direct manager of the Bank’s employee), and to propose them for approval to the Management Board of the Bank;

6) to control the fulfilment terms of tasks approved by the Management Board of the Bank, which are related to the processing of Data or the protection of Data, and to report on the fulfilment of tasks to the Management Board of the Bank;
7) to notify Data breaches to the Supervisory Authority and the Data Subject in the cases and pursuant to the procedures determined in the Bank's "Data Security Breach Investigation Procedure".

3.2. **Functions of the Commission.**

3.2.1. The Commission is a permanent collegial institution approved by the Management Board of the Bank, which fulfils its functions in accordance with the Bank's "Regulation on the Data Protection Commission", including the following:
1) the comprehensive investigation of Data breaches and other incidents related to the security of processing of Data and timely notification to the Management Board of the Bank, the Supervisory Authority and the Data Subject pursuant to the procedures laid down in BRD;
2) the implementation of technical and organisational measures of Data protection, which would enhance the security of processing of Data by the Bank;
3) the assessment of BRD in the field of Data protection, as well as proposing the development and improvement of additional regulatory framework;
4) the preparation of an informative material on the processing of Data by the Bank and the provision of support to other structural units of the Bank, preparing replies to the applications and complaints of Data Subjects in the field of Data protection;
5) the organisation and implementation of the Data Processing Impact Assessment.

3.2.2. In order to ensure the observance of requirements for the prevention of a conflict of interests, the Bank shall ensure that the Commission receives no instructions with regard to the performance of the tasks determined in these Regulations, the Bank's "Regulation on the Data Protection Commission" and other BRD.

## 4. Provisions for the Processing of Data

4.1. **Commencing the Processing of Data.**

4.1.1. The Bank shall ensure that the processing of Data is carried out only for the purposes provided for in Clause 11.1 of the Bank's "Privacy Policy".

4.1.2. If it is necessary to commence the processing of Data for a new purpose, prior to commencing the processing of Data the Bank shall:
1) assess and determine the nature, extent, context and purpose of processing of Data, preventing the processing of Data without the preliminarily determined purposes;
2) assess and determine the legal basis for the processing of Data;
3) determine the risk degree of processing of Data and assess the need to perform the Data Processing Impact Assessment;
4) prepare an informative material to the Data Subject.

4.1.3. Prior to commencing the processing of Data, the Bank shall provide information to the Data Subject free of charge regarding the processing of Data by the Bank in accordance with the provisions of Clause 7.2 of the Bank's "Privacy Policy". The Bank shall ensure that the referred to information has been prepared in a concise, transparent and intelligible manner, explaining in plain and clear language.

4.1.4. The Bank shall publish the information to be provided pursuant to the procedures laid down in Clause 4.1.3 of these Regulations on the Bank's website www.pnbbanka.eu in the section "Privacy Policy". The Data Subject may request and receive information in hard copy at any client service centre of the Bank.

4.2. **Processing of Data.**

4.2.1. During the processing of Data, the Bank shall constantly monitor that the processing of Data by the Bank complies with the principles of processing of Data included in the Bank's "Privacy Policy". The Bank shall be responsible for ensuring that the processing of Data implemented thereby is:
1) lawful, fair and transparent;
2) carried out for specific, explicit and legitimate purposes;
3) carried out on Data compliant in terms of amount and content, preventing the obtaining of excessive Data from the Data Subject;
4) aimed at the accurate processing of Data, timely ensuring the rectification of inaccurate Data;
5) termed in terms of Data storage, which would prevent the processing of Data for longer than is necessary for the purposes for which the Data are processed;
6) performed by appropriate technical and organisational measures relating to Data security and protection to ensure the protection of Data against the authorised or unlawful processing of Data and against the accidental loss, destruction of, or damage to, Data.

4.2.2. In order to vividly prove that the Bank implements the processing of Data in accordance with the provisions of Clause 4.2.1 of these Regulations, the Bank shall introduce and maintain the accountability system, which shall include the following:
1) the exercising of the right of access by the Data Subject;
2) the implementation of the Data Processing Impact Assessment, if planned activities relating to the processing of Data are likely to result in a high risk to the rights and freedoms of the Data Subjects;
3) the timely detection and comprehensive investigation of security incidents relating to the protection of Data, as well as the notification of Data breaches to the Supervisory Authority and the Data Subject;

4) the implementation of planned cooperation with service providers which provide financial and other services on behalf of the Bank or ensure the processing of Data by order of the Bank;
5) the maintenance of the Data Processing Register and ensuring its availability to the Supervisory Authority;
6) the regular training of Bank's employees and assessing the lawfulness of processing of Data and the compliance of the Data protection system.

4.3. **Exercising of the Right of Access by the Data Subject.**

4.3.1. The Bank shall accept applications from the Data Subject on the exercising of the following rights:
1) to access to his or her Data;
2) to rectify his or her Data;
3) to erase his or her Data;
4) to restrict the processing of his or her Data;
5) to receive and send his or her Data (including through the intermediary of the Bank, if technically feasible) provided to the Bank;
6) to object to the processing of his or her Data;
7) to invite to revise automated individual decisions (including with regard to profiling).

4.3.2. The progress of applications of Data Subjects referred to in Clause 4.3.1 of these Regulations, received by the Bank, shall be ensured pursuant to the document circulation procedures laid down in the Bank's "Record-keeping Procedure".

4.3.3. The Data Subject may submit an application on the exercising of the rights provided for in Clause 4.3.1 of these Regulations:
1) in person in paper form at any client service centre of the Bank, ensuring that the application is signed;
2) by post (including courier post) in paper form to the Bank's correspondence address: Riga, 15-2 Elizabetes Street, LV-1010, ensuring that the application is signed;
3) in the form of an electronic document to the Bank's official e-mail address info@pnbbanka.eu, ensuring that the application is signed in accordance with the requirements of laws and regulations in field of preparation of electronic documents;
4) by submitting in the form of an electronic order, using the Bank's automated system for remote access to the account PNB Internetbanka, if such is connected for the Data Subject.

4.3.4. In the event an application is submitted by a third party on behalf of the Data Subject in the form stipulated by Clause 4.3.3(1) of these Regulations, a power of attorney shall be enclosed to the application.

4.3.5. Where there are founded suspicions regarding the identity of the Data Subject who submits the application to the Bank regarding the exercising of the rights referred to in Clause 4.3.1 of these Regulations, the Bank may request to provide additional information necessary for confirming the identity of the Data Subject.

4.3.6. Where the request referred to in the application of the Data Subject applies to a large amount of information to be processed, the Bank shall have the right to request the Data Subject to clarify the amount of his or her request, specifying as to which information and the exercising of which rights of the Data Subject or the processing of Data the request applies.

4.3.7. The Bank shall fulfil the request referred to in the application of the Data Subject without undue delay, no later than within one month following the receipt of the request. In fulfilling the request referred to in the application of the Data Subject, the Bank shall inform the Data Subject of activities carried out with regard to the request.

4.3.8. The maximum term referred to in Clause 4.3.7 of these Regulations for the fulfilment of the request may be extended by 2 (*two*) further months, taking into account the complexity and number of the requests. The Bank shall inform the Data Subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

4.3.9. The Bank shall have the right to fulfil the request referred to in the application or determine and request a charge for the fulfilment of the request, which shall include administrative costs relating to the provision of information or communication or the performance of the requested operation, if the requests of the Data Subject are unfounded or excessive (for example, repeating several times).

4.3.10. Where the Bank does not fulfil the request specified in the application of the Data Subject with regard to the exercising of rights, including in the case referred to in Clause 4.3.9 of these Regulations, the Bank shall inform the Data Subject, without delay and not later than within one month following the receipt of such request, of the causes for the non-fulfilment of the request specified in the application with regard to the exercising of rights and of the possibility of lodging a complaint to the Supervisory Authority.

4.3.11. Where the Data Subject has submitted his or her application with a request in electronic form, the Bank shall provide the information referred to in Clauses 4.3.7, 4.3.8 and 4.3.10 of these Regulations to the Data Subject in electronic form, except if the Data Subject requests otherwise. Where the fulfilment of the referred to request is related to the sending of such information to the Data Subject, which contain Data or another type of confidential information, the Bank shall transfer the information provided in electronic form to the Data Subject in a safe manner, observing the requirements of laws and regulations in the field of security of information systems.

4.3.12. Where the Data Subject has submitted his or her application with a request in paper form, the Bank shall provide the information referred to in Clauses 4.3.7, 4.3.8 and 4.3.10 of these Regulations to the Data Subject to the Data Subject's correspondence address, unless the Data Subject requests otherwise. Where the fulfilment of the referred to request is related to the sending of such information to the Data Subject, which contains Data or another type of confidential information, the Bank shall transfer the provided information in the form of a registered item, if the confirmation of the Data Subject's identity does not require additional information. Where the Bank has founded suspicions with regard to the identity of the Data Subject, the Bank shall transfer the information to be provided to the

Data Subject in person at a client service centre of the Bank, in which the Data Subject is served, or at another client service centre of the Bank, specified by the Data Subject in advance.

4.3.13. In performing operations relating to the exercising of the rights referred to in the application of the Data Subject, the Bank shall immediately inform third parties of necessary changes in the processing of Data in the cases referred to in the Bank's "Privacy Policy".

4.4. **Right of Access by the Data Subject to His or Her Data.**

4.4.1. Where the Bank receives an application of the Data Subject on the exercising of the right specified in Clause 4.3.1(1) of these Regulations, the Bank shall ensure the Data Subject of a possibility of receiving the following information:

1) the purpose of processing of Data;
2) the relevant category of Data;
3) the recipient of Data or the category of recipients to whom the Data are disclosed or will be disclosed, in particular on recipients in third countries or international organisations (if Data are sent to a third country or international organisation, the Data Subject shall have the right to receive information on the relevant safeguards applied with regard to the sending of Data);
4) if possible, the planned period of Data storage, or, if impossible, criteria used to determine that period;
5) the existence of the right to request from the Bank rectification or erasure of the Data of the Data Subject, or restriction of processing of Data, or the right to object to such processing of Data;
6) the right to lodge a complaint with the Supervisory Authority;
7) all the available information with regard to the source of Data, if Data are not collected from the Data Subject;
8) the existence of automated decision-making, including profiling, and meaningful information for the Data Subject about the logic involved, as well as the significance and the envisaged consequences of such processing for the Data Subject.

4.4.2. The rights referred to in Clause 4.4.1 of these Regulations shall be personalised and be granted to the Data Subject regardless of the amount of information which he or she had or is available in accordance with Clause 4.1.3 of these Regulations. Simultaneously, the Bank shall provide the information referred to in Clause 4.4.1 of these Regulations, observing the principles of providing information as referred to in Clause 4.1.3 of these Regulations.

4.4.3. The Data Subject, exercising the right to access to his or her Data, shall have the right to request and receive a copy of his or her Data being processed by the Bank. That right can be exercised with regard to Data, rather than to documents. The Bank shall not issue documents or copies of documents to the Data Subject, except if the Data Subject is able to justify the particular need to receive a copy of the document (for example, if only the content and form of the document enable to draw conclusions on the significance of Data and possible consequences which such processing of Data can cause for the Data Subject).

4.4.4. The right to receive a copy of his or her Data being processed by the Bank, being exercised by the Data Subject, may not have an unfavourable impact on the rights and freedoms of other persons. In the event a copy of requested information contains the Data of another person in addition to the Data of the relevant Data Subject, the Bank shall have the right to not issue a copy of information.

4.4.5. For all the additional copies requested by the Data Subject, the Bank may collect a charge based on administrative costs.

4.5. **Right to Restrict the Processing of Data by the Data Subject.**

4.5.1. Where the Bank receives an application of the Data Subject on the exercising of the right specified in Clause 4.3.1(4) of these Regulations, the Bank shall assess whether there is any of the conditions referred to in Clause 7.6 of the Bank's "Privacy Policy" for discontinuing the processing of Data of the Data Subject, if necessary, requesting the Data Subject to provide additional information serving as grounds for the request.

4.5.2. Where there is any of the conditions for discontinuing the processing of Data of the Data Subject, the Bank shall discontinue the processing of Data of the Data Subject (except storage), if necessary, clarifying the amount of the Data Subject's request, and decide on activities to be carried out to fulfil the request and lift the restriction on the processing of Data.

4.5.3. Prior to lifting the restriction on the processing of Data, the Bank shall inform the Data Subject in accordance with the Regulations of Clause 4.3.11 or 4.3.12 of these Regulations.

4.5.4. Discontinuing the processing of Data of the Data Subject referred to in Clause 4.5.2 of these Regulations shall not be implemented if the Bank processes Data for important reasons of public interest or the establishment, exercise or defence of legal claims of the Bank or for the protection of the rights of another natural or legal person. In the case referred to in this Clause, the Bank shall consider possible activities to be carried out to eliminate unfavourable consequences serving as grounds for the request of the Data Subject.

4.6. **Right to Data Portability by the Data Subject.**

4.6.1. Where the Bank receives an application of the Data Subject on the exercising of the right specified in Clause 4.3.1(5) of these Regulations, the Bank shall assess and, if necessary, determine the amount of the request and fulfil the request with regard to the following Data:

1) Data submitted by the Data Subject him- or herself;
2) Data processed based on the consent of the Data Subject or a contract entered into by and between the Data Subject and the Bank;
3) Data processed by the Bank by automated means;
4) Data without an adverse effect on the rights and freedom of other persons;
5) Data, the processing of which does not apply to the task carried out by the Bank in the public interest or in the exercise of official authority vested in the Bank.

4.6.2. The Bank shall prepare and transfer the requested Data to the Data Subject in the form of an XML sheet which shall comply with the structured, commonly used and machine-readable format determined in Clause 7.7.2 of the Bank's "Policy Privacy". The Data Subject shall have the right to request for preparing and transferring the Data thereto in another machine-readable format, and the Bank shall fulfil such request, unless it is unfounded or excessive and technically impossible.

4.6.3. The Bank shall transfer the Data to be provided in electronic form to the Data Subject in a secure manner, observing the requirements of laws and regulations in the field of security of information systems. Upon the request of the Data Subject, the Bank shall transfer Data directly to another controller (the recipient of Data specified by the Data Subject), if it is technically feasible and complies with BRD requirements in the field of information security and protection.

4.6.4. Upon receiving Data from another controller, the Bank shall responsibly assess the amount of received Data, specifying within its compass the minimum necessary amount of Data for the provision of the relevant services of the Bank before the Data Subject uses the right to Data probability with another controller. If the Bank, within the framework of portability, has received more information than is necessary for providing its service, the Bank shall erase excessive information or, if it is impossible due to the nature of information and the link to the Data Subject, use this information only for the purposes specified by the Data Subject.

4.7. **Right to Object by the Data Subject to the Processing of Data.**

4.7.1. If the Bank receives an application of the Data Subject on the exercising of the right specified in Clause 4.3.1(6) of these Regulations, the Bank shall establish the amount of the request and whether the processing of Data referred to in the request is based on Point (e) or (f) of Article 6(1) of the Regulation.

4.7.2. If the legal basis for the processing of Data is one of those referred to in Clause 4.7.1 of these Regulations, the Bank shall establish the basis of the request, which includes information provided by the Data Subject regarding the infringed interests, rights and freedoms of the Data Subject. After establishing information referred to in this Clause, the Bank shall assess and decide whether the legitimate interests pursued by the Bank in the processing of Data override the interests, rights and freedoms of the Data Subject.

4.7.3. If the Bank establishes the circumstances that confidently suggest that the legitimate interests pursued by the Bank in the processing of Data override the interests, rights and freedoms of the Data Subject, the processing of Data of the Data Subject is necessary for the Bank for the establishment, exercise or defence of legal claims, the Bank shall have the right to refuse from fulfilling the request.

4.7.4. Conditions referred to in Clauses 4.7.1, 4.7.2 and 4.7.3 of these Regulations shall not apply to the examination of a request, if the Data Subject objects to the processing of his or her Data for the needs of direct marketing.

4.8. **Rights of the Data Subject with Regard to Automated Individual Decision-Making.**

4.8.1. If the Bank receives an application of the Data Subject on the exercising of the right specified in Clause 4.3.1(7) of these Regulations, the Bank shall assess and, if necessary, establish the amount of the request, and take appropriate measures in order to protect the rights and freedoms and legitimate interests of the Data Subject, ensuring the revision of an automated individual decision.

4.8.2. The Data Subject shall have the right to contest any automated individual decision made by the Bank in relation to him or her, except for the following cases:

1) if such decision is allowed and made in accordance with laws and regulations;
2) if the Data Subject has consented to the content of a particular decision by active operations (for examples, entered into a contract);
3) if the Data Subject has not exercised his or her right to contest a particular decision within the term specified by the Bank and the decision has entered into force.

4.8.3. In revising an automated individual decision, the Bank shall ensure the participation of the Bank's employee in the making of an individual decision. The process of making a repeated individual decision shall be organised without undue delay, observing the full guaranteeing of the legitimate interests of the Data Subject. A decision made pursuant to the procedures laid down in this Clause shall be final and not subject to appeal.

4.8.4. The Bank shall not restrict the right of the Data Subject to express his or her opinion on the contested automated individual decision before the Bank makes a repeated individual decision with the participation of the Bank's employee. The right to express an opinion, non-exercised by the Data Subject, shall not be grounds for contesting the repeatedly made individual decision.

4.9. **Performance of the Data Processing Impact Assessment.**

4.9.1. The Bank shall perform the Data Processing Impact Assessment in the following cases:

1) the risk of impact of a new or significantly modified Bank's product or service, within the framework of which the processing of Data of the Data Subject is performed, on Data protection is crucial or high. The level of Data protection impact risk shall be determined pursuant to the procedures laid down in the Bank's "Procedure for Assessing the Risks of New and Significantly Modified Products";
2) if the Bank plans to start the kind of processing of Data, which is included on the list of the Supervisory Authority in accordance with Article 35(4) of the Regulation;
3) if the Bank plans to start a systematic and extensive evaluation of personal aspects of the Data Subject which is based on the automated processing of Data, including profiling, and on which decisions are based that produce legal effects concerning the Data Subject or similarly significantly affect the Data Subject;
4) if the Bank plans to start processing on a large scale of Special Categories of Data;
5) if the Bank plans to start a systematic monitoring of a publicly accessible area on a large scale.

4.9.2. Data Processing Impact Assessment shall be performed in accordance with the Bank's ''Procedure for Data Protection Impact Assessment and Assessment of Bank's Legitimate Interests in the Processing of Data". The

performance of the Data Processing Impact Assessment shall be supervised by the Commission consulting with the Officer. The Commission may perform the Data Processing Impact Assessment also in other cases which are not referred to in Clause 4.9.1 of these Regulations.

4.9.3. The Bank may not perform the Data Processing Impact Assessment prior to commencing the processing of Data, if planned Data processing activities are likely to result in a high risk, in the following cases:

1) if the Bank plans to start the kind of processing of Data, the legal basis for which is compliance with a legal obligation in laws and regulations or the performance of a task carried out in the public interest;
2) if the Bank plans to start the kind of processing of Data, which is included on the list of the Supervisory Authority in accordance with Article 35(5) of the Regulation;
3) if the type, nature, scope, context and purposes of processing of Data planned by the Bank are similar to those of the processing of Data for which the Data Processing Impact Assessment has already been performed.

4.10. **Data Processing Register**

4.10.1. The Bank shall register activities carried out with Data (i.e., processing of Data) in the Data Processing Register. That register shall include information in accordance with the provisions of Clause 5.2 of the Bank's "Privacy Policy".

4.10.2. Where the Bank performs the processing of Data as a processor (Article 4(8) and Article 28 of the Regulation), the Bank shall register all the categories of activities carried out by another controller with Data. In the case referred to in this Clause, the Data Processing Register shall include the following information:

1) the name and contact details of the Bank, the name, surname and contact details of its Officer;
2) the name and contact details of another controller, by whose order the Bank processes Data; the name, surname and contact details of its data protection officer;
3) activities carried out with Data on behalf of another controller (i.e., processing of Data);
4) information on the transfer of Data to a third country or international organisation, including the identification of this third country or international organisation, and, in the case of transfers referred to in the second sub-paragraph of Article 49(1) of the Regulation, the documentation of suitable safeguards;
5) a general description of the technical and organisational security measures.

4.10.3. The Data Processing Register created by the Bank shall be maintained by the Officer, carrying out the following activities:

1) ensuring the inclusion, deletion, editing or supplementing of information referred to in Clause 5.2 of the Bank's "Privacy Policy" and Clause 4.10.2 of these Regulations in the Data Processing Register;
2) ensuring the provision of information from the Data Processing Register at the request of Bank's employee, as well as clarifying information included in the Data Processing Register;
3) ensuring the availability of information included in the Data Processing Register to the Supervisory Authority at the request thereof;
4) organising the monitoring of processing of Data by the Bank with the aim to maintain full information to be included in the Data Processing Register.

4.10.4. The Bank shall maintain the Data Processing Register in electronic format.

4.11. **Processing of Data for Pre-determined Purposes**

4.11.1. The Bank shall carry out the processing of Data according to the pre-determined purposes relating to the attainment of Bank's commercial goals and stipulated by Clause 11.1 of the Bank's "Privacy Policy". The purposes of processing of Data by the Bank shall include the following, inter alia:

1) decision-making on the provision of Bank's services to the Data Subject who is a Bank's client as well as the conditions of Bank's services (including the processing of Data before entering into a Bank's service agreement);
2) entering into a Bank's service agreement or ensuring the performance thereof as well as the assessment of solvency and financial risks of the Data Subject who is a Bank's client, and administration of outstanding payments;
3) the administration of a Bank's service agreement, within the framework of which the Bank has the right to approve transactions and activities carried out based on the Bank's service agreement, to update Data received from the Data Subject who is a Bank's client, to prepare the lists of Data of the Data Subject who is a Bank's client, to collect debts;
4) fulfilling requirements necessary for risk management and mitigation, performing risk management and mitigation, and drafting reports;
5) adherence to prudential requirements, including capital and liquidity requirements applicable to the Bank;
6) assessing the qualification of the Data Subject who is a Bank's client, using collected Data and financial information of the Data Subject who is a Bank's client;
7) analysing and forecasting the habits of the Data Subject who is a Bank's client in order to provide special offers or the most suitable service to the Data Subject who is a Bank's client;
8) assessing the quality of Bank's services provided to the Data Subject who is a Bank's client, including using voice records and carrying out the surveys of the Data Subject who is a Bank's client;
9) the organisation of statistical studies and analysis on market shares and other financial indicators that apply to the groups of Data Subjects who are Bank's clients, Bank's products and services;
10) the development and implementation of Bank's information systems;
11) the right of protection of legitimate interests pursued by the Bank, if the legitimate interests and rights of the Bank have been violated or contested (for example, to send Data to the Bank's legal counsel);

12) the monitoring of territories, premises and their surroundings used by the Bank, using surveillance equipment, as well as the storage of results of surveillance activities in digital form.

4.11.2. The Bank shall periodically revise the determined purposes of processing of Data and the associated kinds of processing of Data in order to establish cases when a purpose or a method of processing of Data is no longer necessary as a result of changes to actual circumstances.

4.11.3. If the Bank needs to use Data for a purpose other than the initial purpose for which the Data have been collected, the Bank shall verify the compatibility of a new purpose with the initial purpose, reassess the legal basis, if the purpose is not compatible with the initial purposes, and ensure the informing of the Data Subject about the change of purposes and the rights of the Data Subject in this regard (for example, the right to object by the Data Subject to the processing of his or her Data for a new purpose). Simultaneously, the Bank shall assess whether it is not required to amend the valid Bank's service agreement with the Data Subject or to enter into a new Bank's service agreement which would ensure the appropriate legal basis for the processing of Data in the event of changes to the purposes.

4.11.4. Prior to commencing the processing of Data for any new purpose or changes to the purpose, the Bank shall receive an opinion from the Officer. If the opinion of the Officer differs and the further processing of Data is carried out contrary to the Officer's instructions, the Bank shall document the grounds for such processing of Data.

4.12. **Categories of Data.**

4.12.1. The Bank shall process Data included in the following categories:

1) basic (including identification) Data, such as:
   - name, surname, personal code, date of birth,
   - identification document data, citizenship, nationality,
   - image, language of communication,
   - contact information (e.g., phone number, address, e-mail address),
2) Data describing behaviour and habits, such as:
   - information on the knowledge and experience of the Data Subject (e.g., in the field of investment),
   - information on activities and the origin of funds (e.g., Data on the employer, business partners, business activities);
3) financial Data, such as:
   - basic information on current account or card, ATM notifications;
   - information on income and assets of the Data Subject;
   - information on obligations, previous payment experience of the Data Subject (including debts);
   - information on transactions on the Data Subject's account and other transactions;
4) electronic and telecommunications Data, including:
   - Client identification information;
   - electronic and telecommunications traffic data;
   - location data (e.g., IP address);
   - electronic and telecommunications content;
5) Data on authentication details (e.g., username, password, PIN code);
6) Data received with the aim of fulfilling legal duties specified in the applicable law (e.g., information obtained upon the request of investigative bodies, tax institutions, court bailiffs);
7) Special Categories of Data (e.g., information on politically exposed persons).

## 5. Duties and Liability of the Responsible Employee

5.1. **General Duties of the Responsible Employee in Carrying out the Processing of Data.**

5.1.1. The Responsible Employee shall process Data observing the confidentiality requirements laid down in BRD. The Responsible Employee shall respect and justify the trust shown by the Bank and the Data Subject, carefully treat the use of Data entrusted thereto, the processing and storage of Data, ensuring the security and confidentiality of entrusted information.

5.1.2. The Responsible Employee, at his or her workplace and fulfilling job duties, shall eliminate to the extent possible the risk of Data coming to the disposal of an unauthorised person, which may occur due to the actions of the Responsible Employee: error, theft, negligence in the transfer of information or the incorrect use of equipment.

5.1.3. The voluntary processing of Data and the use of Data for personal needs shall be prohibited. The Responsible Employee shall carry out the processing of Data only within the framework of fulfilment of his or her direct job duties, observing the accountability duty. Within the framework of the accountability duty, the Responsible Employee shall, at the request of the responsible Bank's official (for example, a Member of the Management Board, head of the Bank's structural unit, the Officer or a Member of the Commission), have a duty to vividly show as to within the framework of which job duties and fulfilling which tasks the particular Data are processed.

5.1.4. Upon detecting a Data breach, the Responsible Employee shall:

1) notify the detected Data breach in accordance with the provisions of the Bank's "Data Security Breach Investigation Procedure";
2) register the operational risk pursuant to the procedures laid down in BRD in the field of operational risk management.

5.1.5. The Responsible Employee shall have a duty to cooperate with the Officer and the Commission in all matters concerning the lawfulness of processing of Data and Data security (protection).

5.1.6. The Responsible Employee shall have a duty to participate in training organised and implemented by the Bank in order to improve the level of knowledge and understanding of Responsible Employees with regard to the matters of Data processing lawfulness and protection.

5.2. **Liability of the Responsible Employee.**

5.2.1. The Responsible Employee shall be liable for the observance of the procedures laid down in these Regulations with regard to the processing of Data, including ensuring the lawful and fair processing of Data. The Responsible Employee, who ensures the servicing of Data Subjects who are Bank's clients, shall be liable for the informing of the Data Subject of his (her) rights.

5.2.2. The Responsible Employee shall be liable for the observance of security requirements laid down in BRD in the field of use of Bank's information systems and confidential information circulation.

5.2.3. The Responsible Employee shall be liable for the observance of the following technical measures relating to the protection of Data:

1) all e-mail letters which contain Data and are sent outside the Bank shall be encrypted;
2) in cases where Data are sent by fax, the recipient shall be informed about the transfer of Data;
3) if Data are prepared for transfer in paper form, they shall be transferred in a closed item — directly to the recipient, or sent in the form of a registered postal item or by courier post;
4) Data shall not be processed outside job duties without authorisation and if a third party requires access to Data, such access shall be granted by the responsible Bank's official pursuant to the procedures laid down in BRD;
5) Data shall not be transferred to third parties without appropriate protection and without the permission of the responsible Bank's official;
6) any hard copies or any electronic copies of documents containing Data, which are stored in a physical and portable format, shall be stored in a secure manner — for example, in lockable cabinets, lockable drawers, lockable premises, etc.;
7) Data shall be processed in a secure manner, without leaving them unattended and preventing their unauthorised processing;
8) if Data are viewed on the computer screen and the relevant computer is left unattended for a certain time, the user shall ensure that the access to the computer (or screen) is blocked;
9) if the copies of documents containing Data (for example, printouts or electronic duplicates) are no longer necessary for work, they shall be destroyed or erased. Paper documents shall be shredded, while electronic documents shall be erased pursuant to the procedures laid down in BRD;
10) Data shall not be stored on portable devices (inter alia, laptops, tablets, smartphones, USB drives, etc.), regardless of whether these devices are owned by the Bank or belong to the user, except for cases when the use of these devices and the processing of Data on them is authorised pursuant to the procedures laid down in BRD, strictly observing instructions and restrictions, but for no longer than is necessary;
11) Data cannot be transferred to another device which belongs to the Bank's employee (except case when the use of such devices and the processing of Data on them is authorised pursuant to the procedures laid down in BRD), and Data may be transferred to the Bank's representative, intermediary, counterparty or another third party who carries out the processing of Data on behalf of by order of the Bank, if the relevant person has consented to fully observe the requirements relating to the secure processing of Data set forth in BRD, as well as has taken all necessary technical and organisational measures for ensuring Data security;
12) all passwords used to protect Data from authorised access shall be changed on a regular basis, and passwords shall be created and stored in accordance with the security requirements set forth in BRD.

5.2.4. If the Responsible Employee does not observe these Regulations and other BRD in the field of Data processing lawfulness and protection, use of Bank's information systems, or orders issued by the Bank on the processing of Data and other confidential information, the Bank shall examine the matter concerning the disciplinary punishment of the Responsible Employee. The assessment of the Responsible Employee's disciplinary liability and the possible application of disciplinary punishment shall be ensured pursuant to the procedures laid down in the Procedure for Disciplinary Liability of Bank's Employees".

5.2.5. The violation of these Regulations and other BRD in the field of Data processing lawfulness and protection, in the field of use of Bank's information systems and circulation of confidential information, or orders issued by the Bank on the processing of Data and other confidential information, which is implemented posing a threat to the integrity and confidentiality of Data, shall be considered as gross violation of an employment contract or another contract between the Bank and the Bank's employee and the internal regulations of the Bank, as a result of which the Bank has the right to terminate employment relationship or other relationship with the Responsible Employee, commencing the employment contract or terminating another contract.

## 6. Related Documents

6.1. 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 (General Data Protection Regulation).

6.2. Personal Data Protection Law of the Republic of Latvia.

6.3. Bank's "Privacy Policy".

6.4. Bank's "Regulation on the Data Protection Commission".

6.5. Bank’s “Procedure for Data Protection Impact Assessment and Assessment of Bank’s Legitimate Interests in the Processing of Data”.
6.6. Bank’s “Procedure for the Risk Assessment of New or Significantly Modified Products”.
6.7. Bank's “Data Security Breach Investigation Procedure”.
6.8. Bank’s “Record-keeping Procedure”.
6.9. Bank’s “Procedure for Creation and Maintenance of the Database of Operational Risk Incidents”.
6.10. Bank’s “Procedure for Disciplinary Liability of Bank’s Employees”.
6.11. Bank’s “Deed of Commitment on Non-disclosure of Business Secret and Official Secret”.
6.12. Bank’s “Data Protection Impact Assessment”.

* * *