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

PRIVACY POLICY

Contents

1. Goal

1.1. The goal of this Policy is the following:

1.1.1. to ensure the processing of Data by the Bank in compliance with the requirements of the Regulation;

1.1.2. to determine the duties of the Bank with regard to the lawfulness of processing and protection of personal data, as well as the rights of Data Subjects with regard to the processing of their personal data in accordance with the Regulation.

1.2. This Policy and general principles included therein shall be observed by all the officials of the Bank, structural units and their employees, as well as service providers, if they provide financial or other services on behalf of the Bank or ensure the processing of Data of Data Subjects by order of the Bank.

2. Terms and Abbreviations Used

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

2.2. **Data Subject** – a 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), 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 client or potential client/legal person, or another third party who is directly or indirectly related to the client.

2.3. **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).

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

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

2.6. **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.

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

2.8. **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.

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

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

3. General Provisions

3.1. This Policy lays down the procedures which the Bank shall observe in processing the Data of Data Subjects. The procedures and principles relating to the processing of Data laid down in this Policy shall be observed by all the parties and persons involved in the processing of Data.

3.2. In implementing the provisions of this Policy, the Bank shall undertake to observe the requirements of laws and regulations, as well as the best practice based on laws and regulations, highly valuing the correct, lawful and fair processing of all types of data, which shall be implemented observing the rights, privacy and trust of Data Subjects to the activities implemented by the Bank.

3.3. The Bank shall revise this Policy and other BRD developed and approved for the implementation of this Policy at least once a year.

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

3.5. This Policy shall apply to the processing of Data wholly or partly by automated means and the processing of Data other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

4. Principles of Processing Data

4.1. In processing Data, the Bank shall observe the following principles:

4.1.1. Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject;

4.1.2. Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

4.1.3. Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4.1.4. Data shall be accurate and, where necessary, kept up to date; the Bank shall take every reasonable step to ensure that Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

4.1.5. Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Data are processed;

4.1.6. Data shall be processed in a manner that ensures appropriate security of the Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4.2. **Lawful, Fair and Transparent Processing of Data.**

4.2.1. The Bank shall ensure that the processing of Data thereby is lawful, fair and transparent, without an unfavourable impact on the rights of the Data Subject.

4.2.2. The Bank shall process Data within the framework of its functions if and to the extent that at least one of the following applies:

1) the Data Subject has given consent to the processing of his or her Data for one or more specific purposes;
2) the processing of Data is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract;
3) the processing of Data is necessary for compliance with a legal obligation to which the Bank is subject;
4) the processing of Data is necessary for the purposes of the legitimate interests pursued by the Bank or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

4.2.3. In implementing the processing of Data for the purposes arising from the legitimate interests pursued by the Bank or by a third party in accordance with the basis referred to in Clause 4.2.2 (4) of these Provisions, the Bank shall, prior to commencing the processing of Data, assess the impact of such processing of Data on the interests or fundamental rights and freedoms of the Data Subject, in particular taking into account proportionality and balance aspects.

4.2.4. The Bank shall have the right to process Data at the request of the Data Subject or of a third party if and to the extent that at least one of the following applies:

1) the processing of Data is necessary in order to protect the vital interests of the Data Subject or of another natural person;
2) the processing of Data is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Bank.

4.2.5. In implementing the processing of Data for the purposes arising from the basis referred to in Clause 4.2.4(1) or 4.2.4(2) of this Policy, the Bank shall, prior to commencing the processing of Data, assess the legal aspects of such processing of Data, in particular taking into account the validity of a request of the Data Subject or of a third party.

4.2.6. The Bank shall process the Special Categories of Data within the framework of functions thereof if and to the extent that at least one of the following applies:

1) the Data Subject has given explicit consent to the processing of Special Categories of Data for one or more specific purposes;
2) processing is necessary to protect the substantial interests of the public based on the laws and regulations of the European Union or the Republic of Latvia;
3) processing relates to Data which are manifestly made public by the Data Subject;
4) processing is necessary for the establishment, exercise or defence of legal claims of the Bank.

4.3. **Processing of Data for Specific, Explicit and Lawful Purposes.**

4.3.1. The Bank shall collect and process the Data of the Data Subject for the purposes determined in Section 11 of this Policy, obtaining Data from the Data Subject or third parties.

4.3.2. The Bank shall process Data for the specific purposes laid down in Section 11 of this Policy or other purposes clearly permitted by the Regulation. Where Data are obtained from the Data Subject, the Bank shall inform the Data Subject of the purposes for which these Data will be processed during the retrieval of Data. Where Data are obtained from third parties, the Bank shall inform the Data Subject of the purposes for which these Data are processed pursuant to the procedures laid down in Clause 7.2.2(2) of this Policy.

4.4. **Processing of Adequate, Relevant and Limited Data.**

4.4.1. The Bank shall collect and process the Data and to the extent which are necessary for a specific purpose, observing that the Data Subject is informed of the relevant purposes pursuant to the procedures laid down in Clause 4.3 of this Policy.

4.4.2. Where the processing of Data is necessary for a purpose other than that for which the Data are collected, the Bank shall, in order to ascertain whether the processing for another purpose is compatible with the purpose for which the Data are initially collected, take into account, inter alia:

1) any link between the purposes for which the Data have been collected and the purposes of the intended further processing;
2) the context in which the Data have been collected, in particular regarding the relationship between the Data Subject and the Bank;
3) the nature of the Data, in particular whether the Special Categories of Data are processed;
4) the possible consequences of the intended further processing for Data Subjects;
5) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

4.5. **Accuracy and Updating of Data.**

4.5.1. The Bank shall maintain the accuracy of all collected and processed Data. The accuracy of Data shall be verified upon collecting the Data and their up-to-dateness shall be revised on a regular basis. If inaccurate or outdated Data have been detected, the Bank shall immediately carry out necessary activities taking into account particular circumstances in order to update, rectify or erase the relevant Data.

4.6. **Timely Processing of Data.**

4.6.1. The Bank shall not store Data for longer than is necessary for the purpose for which these Data have been collected and processed. The Bank shall ensure the timely circulation of the processed Data between the structural units of the Bank, observing that the Data are processed by a structural unit of the Bank as long as it is necessary for the fulfilment of functions of the relevant Bank's structural unit. The Bank shall ensure that the Data which are no longer necessary for achieving a specific purpose are archived or erased.

4.7. **Secure Processing of Data.**

4.7.1. The Bank shall ensure that all collected and processed Data are stored securely and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage according to the criteria set in Section 12 of this Policy.

5. Accountability

5.1. The Bank shall appoint the Officer whose principal task is to monitor whether the Regulation, other binding laws and regulations in the field of data protection, and the requirements of this Policy are observed. The Data Subject shall have the right to apply to the Officer with regard to all the matters relating to the processing of his or her Data, as well as the exercising of rights stipulated by the Regulation and this Policy.

5.2. The Bank shall maintain the Data Processing Register on all Data, the collection, keeping and processing of which has been implemented by the Bank. The Data Processing Register shall include the following information:

1) the name and contact details of the Bank (the joint controller and the representative, if any);
2) the name, surname and contact details of the Officer;
3) the purposes of processing of Data;
4) a description of categories of Data Subjects on which the Data are collected, kept and processed;

5) the categories of Data which are collected, kept and processed;
6) information on third parties (categories of recipients) who will receive personal Data from the Bank;
7) information on the transfer of Data to a third country;
8) information on the storage terms of Data;
9) a description of technical and organisation measures taken by the Bank to ensure data security.

5.3. The Bank shall ensure the availability of the Data Processing Register to the Supervisory Authority.

6. Data Protection Impact Assessment

6.1. The Bank shall carry out the Data protection impact assessment in all the cases when planned data processing activities — type, nature, scope, context and purpose — are likely to result in a high risk to the rights and freedoms of Data Subjects. The Data protection impact assessment shall apply to the following crucial areas:
1) the purposes of processing of Data and the processing activities carried out;
2) information on the legal basis for the processing of Data by the Bank, including the legitimate interest pursued by the Bank;
3) an assessment of the necessity and proportionality of operations relating to the processing of Data in relation to the purposes;
4) an assessment of the risks to the rights and freedoms of Data Subjects;
5) information on the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure Data protection and to demonstrate compliance with the Regulation and this Policy taking into account the rights and legitimate interests of Data Subjects and of other persons concerned.

6.2. The performance of the Data protection impact assessment shall be supervised by the Commission. At the request of the Commission, the Officer shall provide advices with regard to the Data protection impact assessment.

7. Rights of the Data Subject

7.1. The Bank shall guarantee the Data Subject the following rights with the regard to the processing of his or her Data:
1) to be informed about the processing of Data by the Bank, its lawfulness and his or her rights;
2) to access to his or her Data;
3) to rectify his or her Data;
4) to erase his or her Data;
5) to restrict the processing of his or her Data;
6) to receive and send his or her Data (including through the intermediary of the Bank, if technically feasible) provided to the Bank;
7) to object to the processing of his or her Data;
8) to invite to revise automated individual decisions (including with regard to profiling).

7.1.1. The Data Subject may exercise the rights referred to in Clause 7.1 of this Policy by submitting a request in one of the ways referred to in the Bank's "Personal Data Processing Regulations". The Bank shall reply to such request of the Data Subject without undue delay, observing the information provision procedures and terms determined in the Bank's "Personal Data Processing Regulations".

7.2. **Informing the Data Subject.**

7.2.1. Upon obtaining Data, the Bank shall ensure the provision of the following information to the Data Subject with regard to the processing of his or her Data:

1) the name and contact details of the Bank;
2) the name, surname and contact details of the Officer;
3) the purposes of the processing for which the Data are intended as well as the legal basis for the processing of the Data;
4) in certain cases, the legitimate interests pursued by the Bank, whereon the processing of data is based, as well as the right to object against such processing of Data;
5) information on the categories of collected and processed Data in cases where the Data are not obtained directly from the Data Subject;
6) information on a third party in cases where the Data are transferred to the third party;
7) information on the transfer, including information on security measures, in cases where the Data are transferred to a third party located outside the European Union (see Section 13 of this Policy);
8) information on the period for which the Data will be stored, or if that is not possible, the criteria used to determine that period;
9) information on the rights of the Data Subject and the possibilities of exercising them in accordance with this Policy and other BRD;
10) information on the processing of the Data by the Bank based on the consent of the Data Subject as well as the right to withdraw this consent;
11) information on the right to apply to the Officer with regard to the matters relating to the processing of his or her Data, as well as the exercising of rights stipulated by the Regulation and this Policy;
12) information on the right to lodge a complaint with the Supervisory Authority;
13) information on whether the collection and processing of the personal Data is determined in accordance with statutory or contractual requirements or duties, as well as information on whether the Data Subject is obliged to provide the Data and of the possible consequences of failure to provide such Data;
14) information on automated decision-making using the Data of the Data Subject (inter alia, profiling), including information on how decisions are made as well as on the significance of these decisions and any consequences.

7.2.2. Information referred to in Clause 7.2.1 of this Policy shall be provided to the Data Subject:

1) at the time of obtaining Data, if the Data are obtained from the Data Subject;
2) if Data are not obtained from the Data Subject:
   - within a reasonable period after obtaining the Data, but at the latest within one month, having regard to the specific circumstances in which the Data are processed,
   - if the Data are to be used for communication with the Data Subject, at the latest at the time of the first communication to that Data Subject,
   - if a disclosure of the Data to a third party is envisaged, at the latest when the Data are first disclosed.

7.2.3. Information referred to in Clause 7.2.1 of this Policy shall not be provided if and to the extent the relevant information is already at the disposal of the Data Subject.

7.3. **Right of Access by the Data Subject.**

7.3.1. The Data Subject shall have the right to obtain additional information on his or her Data collected, processed and stored by the Bank.

7.3.2. The Bank shall have the right to ask the Data Subject to adjust his or her request: for instance, to specify the amount of the requested information or the period for which the information is requested.

7.3.3. The Bank shall request no charge from the Data Subject for the processing of a request submitted pursuant to the general procedures and the preparation of necessary information.

The Bank shall reserve the right to request the Data Subject to pay a reasonable charge for additional copies of Data for the information which has already been provided to the Data Subject, fulfilling his or her request, as well as for requests which are obviously unfounded or excessive, in particular, if these requests are repeating and recurrent.

7.4. **Rectification of Data.**

7.4.1. If the Data Subject informs the Bank that the Data at the disposal of the Bank are inaccurate or incomplete, requesting to rectify or complete them, the Bank shall rectify or complete the Data and inform the Data Subject of the rectification of the Data. The Bank shall carry out all activities relating to the rectification or completion of Data without undue delay.

7.4.2. In cases where inaccurate Data are transferred to third parties, the Bank shall inform these third parties of the rectification or completion of the relevant Data, unless this proves impossible or involves disproportionate effort.

7.5. **Erasure of Data.**

7.5.1. The Data Subject shall have the right to request from the Bank the erasure of personal data concerning him or her where one of the following applies:

1) the Data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
2) the Data Subject withdraws consent on which the processing of the Data is based, and where there is no other legal ground for the processing;
3) the Data Subject objects to the processing of the Data for the purposes of the legitimate interests pursued by the Bank or by a third party, and there are no overriding legitimate grounds for the processing of the Data of the Data Subject by the Bank or by the third party;
4) the Data Subject objects to the processing of the Data for the needs of direct marketing;
5) the Data have been unlawfully processed;
6) the Data have to be erased for compliance of the Bank with a legal obligation in laws and regulations to which the Bank is subject.

7.5.2. Where the Bank has no founded reasons for rejecting the erasure of the Data, the Bank shall observe all erasure requests and inform the Data Subject of the erasure of the Data.

7.5.3. Where at the request of the Data Subject, the Bank erases the Data which are transferred to third parties, the Bank shall inform these third parties of the erasure of the Data, unless this proves impossible or involves disproportionate effort.

7.6. **Restriction of Processing of Data.**

7.6.1. The Data Subject shall have the right to request from the Bank restriction of processing where one of the following applies:

1) the accuracy of the personal data is contested by the Data Subject, for a period enabling the Bank to verify the accuracy of the personal Data;
2) the processing is unlawful and the Data Subject opposes the erasure of the personal data and requests the restriction of their use instead;
3) the Bank no longer needs the personal data for the purposes of the processing, but they are required by the Data Subject for the establishment, exercise or defence of legal claims;
4) the Data Subject has objected to the processing for observing the legitimate interest of the Bank or of a third party, pending the verification whether the legitimate grounds of the Bank or of the third party override those of the Data Subject.

7.6.2. Where processing has been restricted at the request of the Data Subject, such Data shall, with the exception of storage, only be processed with the Data Subject's consent or for the establishment, exercise or defence of legal claims of the Bank or for the protection of the rights of another natural or legal person, or for reasons of important public interest of the European Union or of a Member State.

7.6.3. The Data Subject shall be informed by the Bank before the restriction of processing is lifted.

7.6.4. Where at the request of the Data Subject, the Bank restricts the processing of the Data which are transferred to third parties, the Bank shall inform these third parties of the restriction of processing of the Data, unless this proves impossible or involves disproportionate effort. Where the Bank has informed a third party of the restriction of processing of the Data, it shall immediately notify also the removal of the relevant restriction.

7.7. **Data Portability.**

7.7.1. Where the processing of Data is implemented by automated means and based on the consent of the Data Subject or under a contract to which the Data Subject is party, the Data Subject shall have the right to receive a copy of his or her Data and use it for his or her own purposes (namely, to transfer to third parties). The Bank's copy of Data shall not include the data of a third party, if the legitimate interests of the Data Subject do not override the interests or fundamental rights and freedoms of the third party which require protection of personal Data.

7.7.2. In order to ensure Data portability in accordance with the requirements of this Policy, the Bank shall provide a copy of the Data in a structured, commonly used and machine-readable format.

7.7.3. Where technically feasible and where requested by the Data Subject, the Bank shall send a copy of Data directly to the third party specified by the Data Subject.

8. Right to Object to the Processing of Data

8.1. The Data Subject shall have the right to object to the processing of his or her Data, if the processing is based on the legitimate interests of the Bank — including profiling, processing for the needs of direct marketing, scientific research or statistics.

8.2. Where the Data Subject objects to the processing of Data carried out:

8.2.1. based on the legitimate interests of the Bank, the Bank shall immediately discontinue such processing of Data, unless it can prove that the Bank's legitimate purposes of processing override the interests, rights and freedoms of the Data Subject, or the relevant processing is necessary for the establishment, exercise or defence of legal claims of the Bank (for instance, in court, law enforcement authorities, etc.);

8.2.2. for the needs of direct marketing, the Bank shall immediately discontinue such processing;

8.2.3. for the needs of statistical or scientific research, the Bank shall immediately discontinue such processing of Data, except if the processing is necessary for the performance of a task carried out in the public interest.

9. Automated Decision-Making

9.1. The Bank shall process the Data with the aim to make a decision based solely on the automated processing of Data (including profiling), if the automated decision:

1) is necessary for entering into, or performance of, a contract between the Data Subject and the Bank;
2) is authorised by the European Union or Member State law to which the Bank is subject;
3) is based on the Data Subject's explicit consent.

9.2. In cases where the Bank processes Data with the aim to make a decision based solely on the automated processing of Data (including profiling), which produces legal effects concerning him or her or similarly significantly affects him or her, the Bank shall ensure the Data Subject of the right to contest this decision or request a Bank's employee to participate in the making of this decision.

10. Profiling

10.1. In cases where the Data of the Data Subject are processed for the purposes of profiling, the Bank shall observe the following conditions:

1) the Data Subject is provided with clear information on the processing of Data within the framework of profiling, including the significance and possible consequences of such processing;
2) appropriate mathematical calculations and methods or statistical procedures are applied;
3) appropriate technical and organisational measures necessary to reduce the probability of mistakes and enable to easily identify and correct mistakes, if any, are used;
4) all the Data processed within the framework of profiling are provided to prevent any discriminating influence which can occur as a result of profiling.

11. Purposes of Processing of Data

11.1. The Bank shall collect and process the Data of the Data Subject for the following purposes:
11.1.1. the provision of financial services;
1) the provision of investment services, including the opening and maintenance of accounts;
2) the provision of payment services within the meaning of the Law of the Republic of Latvia On Payment Services and Electronic Money;
3) crediting - including in the form of loan, lease, factoring, overdraft or pledge;
4) the provision of investment services and non-core investment services;
5) the performance of trust operations;
6) the lease of individual safes;
7) the issue of guarantees and other deeds of commitment, by which the duty to be liable to a creditor for a third party's debt is undertaken;
8) the maintenance of escrow accounts;
11.1.2. the provision of remote services (for example, SMS Bank, Bank's automated system for remote access to the account via PNB Internetbanka);
11.1.3. the organisation of campaigns, lotteries and similar events (including direct marketing and statistical research events) relating to the advertising of services provided by the Bank;
11.1.4. video surveillance for ensuring the security of visitors and Bank's employees and the Bank;
11.1.5. the performance of activities relating to the fulfilment of duties imposed by laws and regulations (inter alia, performance of activities relating to anti-money laundering and counter-terrorism financing, enforcement of recovery orders).

12. Data Protection Measures

12.1. The Bank shall ensure that all its employees, representatives, intermediaries, counterparties or other third parties who process Data implement technical information protection measures and secure data processing measures determined in this Policy and other BRD on behalf or by order of the Bank.

12.2. In implementing technical information protection measures and secure Data processing measures, the Bank shall ensure the following:
12.2.1. the pseudonymisation and encryption of Data;
12.2.2. the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
12.2.3. the restoration of Data availability and access thereto in a timely manner in the event of a physical or technical incident;
12.2.4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

12.3. The Bank shall ensure that the following organisational measures are taken when collecting, storing and processing Data:
12.3.1. all Bank's employees, representatives, intermediaries, counterparties or other third parties who process the Data on behalf or by order of the Bank:

1) are fully informed about their and Bank's duties with regard to the lawfulness of processing of Data and the fundamental principles of Data protection which are observed in accordance with this Policy and other BRD;
2) are appropriately trained and supervised;

12.3.2. the right to access the Data at the disposal of the Bank is granted only to the Bank's employees, representatives, intermediaries, counterparties or other third parties who process the Data on behalf or by order of the Bank and who require access to and the use of the Data to fulfil their duties;

12.3.3. the methods of collecting, storing and processing the Data are assessed and revised on a regular basis;

12.3.4. the performance of the Bank's employees, representatives, intermediaries, counterparties or other third persons who process the Data on behalf or by order of the Bank in implementing the processing of Data in compliance with this Policy, is assessed and revised on a regular basis;

12.3.5. all Bank's employees, representatives, intermediaries, counterparties or other third persons who process the Data on behalf or by order of the Bank are obliged to observe the lawfulness of processing of Data and Data protection security requirements in accordance with the requirements of the Regulation and this Policy, as well as other BRD;

12.3.6. all representatives, intermediaries, counterparties or other third parties who process the Data on behalf or by order of the Bank ensure that all their employees are subject to the same provisions which Bank's employees must fulfil in accordance with this Policy;

12.3.7. in cases where representatives, intermediaries, counterparties or other third parties who process the Data on behalf or by order of the Bank do not fulfil their obligations determined in this Policy, they compensate the Bank for losses (including losses with regard to claims, legal proceedings, sanctions), which have occurred or may occur as a result of non-fulfilment of the relevant obligations.

13. Transfer of Data to Third Countries

13.1. The Bank shall have the right, for the purposes determined in Clause 11.1 of this Policy, to send (transfer) Data to third countries other than European Union Member States, ensuring that the protection level of fundamental rights of Data Subject guaranteed by the Regulation will not decrease, and prior to transferring the Data, the Bank shall check the compliance of the volume of the Data to be sent (transferred) with the purposes determined in Clause 11.1 of this Policy, in particular taking into account the Data minimisation principle.

13.2. The sending (transfer) of Data to third countries other than European Union Member States shall be permissible:

13.2.1. upon the Bank's initiative, if at least one of the following applies:
1) if the sending (transfer) of Data is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract;
2) if the sending (transfer) of Data is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Bank and another natural or legal person;
3) if the sending (transfer) of Data is necessary for the establishment, exercise or defence of legal claims;
4) if the sending (transfer) of Data is necessary for important reasons of public interest.

13.2.2. at the request of the Data Subject, if the Data Subject has explicitly consented to the transfer of Data and the Bank has informed the Data Subject of the possible risks, if any;

13.2.3. at the request of a third party, if at least one of the following applies:
1) if the Data Subject has explicitly consented to the transfer of Data;

2) if the sending (transfer) of Data is necessary in order to protect the vital interests of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving consent;
3) if the sending (transfer) of Data is necessary for important reasons of public interest;
4) if the European Commission has decided that the third country other than European Union Member State, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of Data protection;
5) if the controller or processor of a third country other than European Union Member State has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

14. Notification of a Data Breach

14.1. All Data breaches shall be immediately notified to the Officer.

14.2. If a Data breach occurs and this breach can pose a threat to the rights and freedoms of the Data Subject (for example, financial losses, confidentiality violations, discrimination, reputational losses or other significant social or economic losses), the Commission or the Officer shall, without undue delay and, where feasible, not later than 72 (*seventy-two*) hours after having become aware of it, notify the Data breach to the Supervisory Authority.

14.3. Where the Data breach can cause a high risk to the rights and freedoms of the Data Subject, the Commission or the Officer shall without undue delay inform the Data Subjects of the rights which have been infringed and the Data breach, except for the following cases:
1) if the Bank has implemented appropriate technical and organisational Data protection measures, and those measures were applied to the Data affected by the Data breach;
2) if the Bank has taken subsequent measures which ensure that the high risk to the rights and freedoms of Data Subjects is no longer likely to materialise;
3) it would involve disproportionate effort, and there shall instead be a public communication or similar measure whereby the Data Subjects are informed in an equally effective manner.

14.4. In the notification referred to in Clause 14.2 of this Policy, the Commission or the Officer shall include the following information:
1) the categories and approximate number of the relevant Data Subjects;
2) categories and approximate number of the relevant Data records;
3) the name, surname and contact details of the Officer;
4) a description of possible consequences of the Data breach;
5) a description of measures taken by or proposed by the Bank to address the Data breach, including, where appropriate, mitigate its possible adverse effects.

15. Related Documents

15.1. 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).
15.2. Personal Data Protection Law of the Republic of Latvia.
15.3. Law of the Republic of Latvia On Payment Services and Electronic Money.
15.4. Bank's "Personal Data Processing Provisions".
15.5. Bank's "Regulation on the Data Protection Commission".

* * *