

## Guidelines for Processing of Personal Data of Individuals

Guidelines for Processing of Personal Data of Individuals, hereinafter – Data Processing Guidelines, shall determine the procedure according to which the Bank processes Personal Data. Data Processing Guidelines shall be applied to the Processing of Personal Data performed by the Bank, including such processing that has been started prior to Data Processing Guidelines entry into force.

More detailed information regarding the Processing of Personal Data may be included into the agreements concluded between the Bank and the Data Subject, into other documents that are binding for the Data Subject, as well as available on the Bank's home page.

### 1. Terms Used:

- 1.1. **Processor** – the Bank's partner (individual or legal entity, enterprise or other separate entity), which pursuant to the written agreement processes Personal Data on behalf and for the benefit of the Bank.
- 1.2. **Bank** – JSC "Reģionālā investīciju banka", registered at the Register of Enterprises of the Republic of Latvia with the reg. No. 40003563375, legal address: 2 J. Alunāna St., Rīga, LV-1010,
- 1.3. **Bank's home page** – the Bank's home page: [www.ribbank.com](http://www.ribbank.com).
- 1.4. **Data Subject** – an individual that established business relations with the Bank or that is related to such business relations, including a Customer – an individual, a Customer's representative, a Real Beneficial Owner, related parties, a guarantor, candidates for job openings advertised by the Bank, a person associated with the Bank, a partner, as well as persons that possessed such status previously or that expressed their willingness in any manner to become ones, or granting them such status is required by the normative acts, or any other identified or identifiable individual whose Personal Data is processed by the Bank.
- 1.5. **Remote Communication Device** – any device, including remote account management tools that can be used without simultaneous physical presence of the payment service provider and the payment service user to conclude agreements between the Data Subject and the Bank, as well as to receive/provide Banking services.
- 1.6. **Customer** – an individual or a legal entity or an association of such persons that uses, used or expressed their willingness to use banking services and/or that acts as a payer or as a beneficiary.
- 1.7. **AML/CFTP Law** – Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing.
- 1.8. **Real Beneficial Owner** – an individual that is the owner of the Customer – legal entity, or that controls the Customer, or on behalf of which, to the benefit of which or in favour of which business relations are established or a random transaction is executed, and which is at least:
  - a) with regard to legal entities – an individual that directly or indirectly owns more than 25% of capital shares or voting shares of a legal entity, or which directly or indirectly controls it;
  - b) with regard to legal arrangements – an individual that owns or in favour of which a legal arrangement is established or operates, or which directly or indirectly controls it, including where it is a founder, an proxy or a manager of such an arrangement;
- 1.9. **Personal Data (Data)** – any data that provides any information regarding the Data Subject, including objectively documentable information (*for example, name, surname, personal identification number, address, telephone number, account number and account information*), as well as subjective information regarding the Data Subject (*for example, credit rating*). Personal Data is also understood to be information documented in any form, i.e. the data documented both in writing in paper form and in electronic format, as audio and video recordings, as well as photo and documented biometric data.

- 1.10. **Personal Data Protection** – a set of measures stipulated by the normative acts that is ensured by the Bank while processing the Personal Data.
- 1.11. **Processing of Personal Data** – any action or a combination of actions performed with the Personal data manually or automatically (*for example, Personal Data collection, registration, organising, structuring, storing, as well as adjusting or transforming thereof, returning, disclosing, restricting, deleting, destroying, etc.*).
- 1.12. **Consent** – Data Subject's consent that is specific, intended, unambiguously and freely expressed by a written or verbal reference to the corresponding person's consent to the Processing of Personal Data to a certain extent and in compliance with the objectives determined by the Bank.
- 1.13. **Profiling** – any kind of automated Processing of Personal Data that is expressed in using Personal Data for the purpose of evaluating specific private aspects related to the Data Subject, especially for the analysis and forecast of aspects in respect of behaviour, financial position, performance of the Data Subject, etc.
- 1.14. **Third Party** – any person that is not the Bank, employee of the Bank, a person directly authorised by the Bank and not a Processor, having their own independent intentions in respect of Processing of Personal Data.
- 1.15. **Third Countries** – territories outside the European Union and the European Economic Area.

## 2. General Provisions

- 2.1. These Guidelines for Processing of Personal Data of Individuals describe in general the way of how the Processing of Personal Data is organised. In addition to these Guidelines, the Processing of Personal Data may be included in agreements as well as other documents related to banking services.
- 2.2. The Bank shall ensure the Processing of Personal Data in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council 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), and the normative acts of the Republic of Latvia and implement appropriate technical and organisational measures for Personal Data Protection.

## 3. Personal Data Categories

The Bank may obtain Personal Data from the Data Subject and within cooperation between the Bank and the Subject, including, as a result of using banking services, as well as from other sources, for example, from various public registers or limited access registers, as well as from Third Parties. The Bank may record phone conversations, take and save photo / video images, save correspondence, and otherwise document the communication of the Data Subject with the Bank.

The Bank may process Personal Data included (but not limited to) in the following Personal Data categories:

- 3.1. identification data (*for example, name, surname, personal identification number, date and place of birth, information about the identity document, etc.*);
- 3.2. contact information (*for example, address, e-mail address, telephone number, etc.*);
- 3.3. information about education and professional experience of the Data Subject;
- 3.4. financial information (*for example, information about the Data Subject's income, as well as about source of income and wealth, property, accounts, liabilities, loans, financial experience, transactions, including transactions in financial instruments, etc.*);
- 3.5. information about persons related to the Data Subject (*for example, Data of the Data Subject's family members, etc.*);
- 3.6. data related to mutual cooperation and banking services (*for example, information about the submitted requests and applications, agreements concluded between the parties and execution thereof, made transactions, payments, etc.*);
- 3.7. data that is obtained/created as a result of fulfilment of obligations stipulated by the normative acts by the Bank (*for example, Data obtained by the Bank as a result of fulfilment of the AML/CFTP Law requirements, Data obtained by the Bank in relation to the requests of government institutions,*

*state officials, supervisory and law-enforcement authorities, Data about the Data Subject's tax residency, etc.);*

- 3.8. data related to communication between the Bank and the Data Subject (for example, Data obtained as a result of communication between the Bank and the Data Subject, including during written communication, telephone conversations, visiting the Bank's premises, the Bank's home page and during communication with the Bank via other channels, etc.);
- 3.9. data related to banking services (for example, performance of agreements, performed transactions, agreements, applications);
- 3.10. audio and video data, for example, the visual material of video surveillance, as well as phone conversation records;
- 3.11. special category data (for example, data about the Data Subject's health, its membership in trade union, etc.).

#### **4. Purposes of Processing of Personal Data**

The Bank may process Personal Data for the following purposes (but not limited thereto):

- 4.1. to ensure personnel management in the Bank;
- 4.2. to provide the banking services, including
  - 4.2.1. to identify a Customer;
  - 4.2.2. to provide account maintenance services (for example, to ensure payments and transfers among the financial institutions, etc.);
  - 4.2.3. to ensure remote banking services (for example, Internet Banking and SMS Banking services, etc.);
  - 4.2.4. to provide lending services (for example, to evaluate creditworthiness and other parameters of a Customer/guarantor/pledgor);
  - 4.2.5. to provide payment card services (for example, to ensure preparation, personalisation and issuance of payment cards, authorisation of transactions with payment cards, transactions processing, transactions monitoring, travel insurance for payment cards, etc.);
  - 4.2.6. to provide investment services (for example, to provide services related to financial instruments, including by telephone, etc.);
- 4.3. to ensure communication with the Data Subject (for example, to send Bank notifications, for telephone communication, etc.);
- 4.4. to implement the Bank's obligations established in the normative acts (for example, regarding Customer/potential customer due diligence, including for Customer/potential customer identification, determination of a Real beneficial owner and politically exposed person, in implementing AML/CFTP Law requirements, etc.);
- 4.5. to ensure data exchange with the government institutions (for example, the Credit Register of the Bank of Latvia, the Bank of Latvia, the State Revenue Service, etc.), investigative and law enforcement authorities, state officials;
- 4.6. for marketing purposes (for example, for commercial messages) based on the consent of the Data Subject, if it is stipulated by the requirements of normative acts. The Bank does not require obtaining the consent of the Data Subject to offer and advertise services on the Bank's website, in the Internet Banking system or mobile application;
- 4.7. to evaluate, manage and eliminate risks;
- 4.8. to take economic and administrative measures (for example, to ensure physical safety and protection of property, exchange of information related to consolidation of the Bank, to ensure cooperation with the Bank's partners, document workflow, archiving, use of translation services, etc.);
- 4.9. to protect and to exercise rights and interests of the Bank (for example, to protect rights and interests of the Bank in courts and other government institutions, for debt recovery and collection measures, for using legal services, transfer (ceding) of the Bank's rights of claim to Third Parties, etc.).

#### **5. Legal Basis of Processing of Personal Data**

The Bank processes Personal Data strictly subject to the existence of legal basis thereof. The following legal reasons for the Processing of Personal Data are possible:

- 5.1. an obligation to process Personal Data of the Data Subject results from the requirements of the normative acts binding for the Bank (fulfilment of legal obligations);
- 5.2. the Processing of Personal Data is required for the provision of banking services, as well as for contractual relationship establishment and implementation;
- 5.3. the Bank has received the Consent of the Data Subject;
- 5.4. the Processing of Personal Data is required for the protection of rights and interests of general safety, society, Third Party, the Bank or the Data Subject;
- 5.5. the Processing of Personal Data is necessary for observing the legitimate interests of the Bank or a Third Party.

## **6. Recipient or Categories of Recipients of Personal Data**

Upon the existence of appropriate legal basis and purposes, the Bank may disclose Personal Data to the Data recipients that are included into the following categories of Data recipients (but not limited thereto):

- 6.1. employees of the Bank;
- 6.2. partners of the Bank (including the Processors)/their employees (*for example, MasterCard Europe Sprl, to which Personal Data may be transferred for the purpose of ensuring provision of payment card services, correspondent bank of the Bank, to which Personal Data may be transferred for the purpose of Payment execution, etc.*);
- 6.3. government institutions, state officials, supervisory and law-enforcement authorities and other institutions and officials (*for example, the Bank of Latvia, to which Personal data can be transferred for the purpose of providing the Bank's reports stipulated by the normative acts, etc.*);
- 6.4. registers (*for example, the Credit Register of the Bank of Latvia, to which Personal data can be transferred for the purpose of fulfilling the Bank's obligations regarding provision of information as stipulated by the normative acts, etc.*);
- 6.5. suppliers and partners that provide services related to exercising of rights and obligations of the Bank, as well as their employees (*for example, legal services providers, to which Personal Data can be transferred for the purpose of ensuring the Bank's rights and interests protection in courts and other government institutions, etc.*);
- 6.6. persons related to Data Subjects (*for example, authorised persons, legal services providers, etc.*);
- 6.7. legal entities included in the Bank's group.

## **7. Personal Data Sending to a Third Country and the Applied Guarantees of Data Protection**

- 7.1. The Bank sends Personal Data to a Third Country if adequate safety measures have been ensured. The Bank assumes that Data sending to a Third Country is lawful where one of the following measures is ensured:
  - 7.1.1. a decision was made by the European Commission that the certain Third Country's territory ensures adequate level of protection;
  - 7.1.2. a cooperation agreement is concluded between the Bank and a Third Party located in a Third Country with the application of standard clauses on Data protection developed by the European Commission;
  - 7.1.3. other activities have been conducted, which, in accordance with the requirements of the normative acts, are considered as adequate safety measures (*for example, application of other approved regulations, codes of conduct, certifications, etc.*).
- 7.2. Where none of the safety measures mentioned in the normative acts exist, Personal Data sending to a Third Country may be implemented only if one of exceptional legal bases specified in the normative acts is applied, for example, but not limited to, a Data Subject has provided its Consent, or Personal Data sending to a Third Country is required for execution of agreements between the Data Subject and the Bank (*for example, Data sending to a correspondent bank located in a Third Country is required for payment execution performed by the Data Subject*).

## **8. Personal Data Storage Period**

- 8.1. The Bank stores Personal Data in accordance with the terms prescribed by the normative acts, and only for as long as that is required for a certain purpose. Nevertheless, the Bank pays attention to the fact that upon reaching the initial objective of Processing of Personal Data, new legitimate objectives for processing of these Personal Data may occur, which may constitute a ground for a longer Personal Data storage period than it had been established originally.

## **9. Rights of Data Subject**

The Bank shall ensure the following rights stipulated by the normative acts for a Data Subject:

### **9.1. Right of Access to One's Personal Data**

#### **9.1.1. Under this right, a Data Subject may:**

- 9.1.1.1. obtain confirmation of its Personal Data processing, i.e. upon the request of a Data Subject to obtain the Bank's response on the fact that Personal Data of the Data Subject are/are not processed;
- 9.1.1.2. obtain access to its Personal Data, i.e. to receive a copy of its Personal Data held by the Bank (not documents);
- 9.1.1.3. receive additional information regarding its Personal Data processing.

- 9.1.2. The Bank shall ensure these rights free of charge, however, the Bank shall have the right to charge fees in accordance with the Bank's Price list or to refuse a request if the Data Subject's request is obviously unreasonable or excessive.

### **9.2. Right to Rectify Personal Data**

- 9.2.1. The Data Subject may request that the Bank without undue delay rectify inaccurate Personal data of the Data Subject held by the Bank.

### **9.3. Right to Transfer Data**

- 9.3.1. The Data Subject shall have the right to receive from the Bank Personal Data about itself for storage thereof and, for example, to transfer it to another service provider. These rights shall relate only to the Personal Data that meet the following parameters:

- 9.3.1.1. Personal Data relates to a certain Data Subject that made a request;
- 9.3.1.2. Personal Data has been provided to the Bank by the Data Subject itself;
- 9.3.1.3. legal basis for the Processing of Personal Data is the Consent or establishment and implementation of contractual relations;
- 9.3.1.4. such Processing of Personal Data is performed by automated means.

- 9.3.2. The Bank shall ensure these rights where this is technically possible and free of charge, however, the Bank shall have the right to charge fees in accordance with the Bank's Price List if the Data Subject's request is obviously unreasonable or excessive.

### **9.4. Right to Be Forgotten**

- 9.4.1. The Data Subject shall be entitled to demand that the Bank without undue delay cease the Processing of Personal Data of the Data Subject and delete it, if:

- 9.4.1.1. Personal Data is no longer needed for implementing the goals for which it had been initially collected or otherwise processed;
- 9.4.1.2. The Data Subject has withdrawn its Consent on the basis of which Personal Data were processed and there is no other legal basis for the Processing of Personal Data.
- 9.4.1.3. The Data Subject objects to the Processing of Personal Data, and after repeated assessment of legitimate interests the Bank admits that no significant legal basis for processing exists, or processing is performed for marketing purposes.

- 9.4.2. The Bank shall have the right not to delete Personal Data in the following cases:

- 9.4.2.1. if the Bank has to continue the Processing of Personal Data under compliance with its legal obligation (obligation on the Processing of Personal Data is established by the normative acts);
- 9.4.2.2. the Processing of Personal Data is required for archiving purposes;
- 9.4.2.3. in other cases upon the existence of corresponding legal basis.

### **9.5. Right to Limit the Processing**

- 9.5.1. The Data Subject shall have the right to require that the Bank in certain cases and for a certain period restrict the Processing of Personal Data of the Data Subject:

- 9.5.1.1. if the Data Subject challenges the accuracy of Personal Data – for a period while the Bank verifies the accuracy of Personal Data;
- 9.5.1.2. if processing is unlawful and the Data Subject objects to Personal Data deletion, instead requesting to limit the use of Personal Data – for a period requested by the Data Subject;
- 9.5.1.3. if the Bank no longer needs Personal Data for processing, but the Data Subject needs it for submission, implementation or protection of legitimate claims – for a period requested and justified by the Data Subject;
- 9.5.1.4. if the Data Subject objects to processing that is based on legitimate interests of the Bank – for a period while it is verified whether the Bank's legitimate interests are more important than legitimate interests of the Data Subject.
- 9.5.2. Prior to lifting restrictions, the Bank informs the Data Subject thereof.

## **9.6. Right to Object**

- 9.6.1. The Data Subject shall have the right to object to the Processing of its Personal Data if it is based on legitimate interests, including Profiling for marketing purposes (direct selling purposes) (for example, receiving commercial messages).
- 9.6.2. The Data Subject shall not have the right to object to processing of the Data if the basis for Data processing is:
  - 9.6.2.1. Consent;
  - 9.6.2.2. establishment or implementation of contractual relations;
  - 9.6.2.3. implementation of legal obligation;
  - 9.6.2.4. protection of vital interests of Data Subject or Third Parties.

## **9.7. Right to Make Individual Automated Decisions**

- 9.7.1. The Data Subject shall have the right not to be subject to fully automated individual decision making, including Profiling, if a decision made in such manner in relation to the Data Subject creates legal consequences or affects Data subject in a similar way. Data subject shall not have the right to refuse such decision making if:
  - 9.7.1.1. the decision is required for conclusion or execution of agreement concluded between the Bank and the Data Subject;
  - 9.7.1.2. decision making is allowed in accordance with the applicable normative acts;
  - 9.7.1.3. the Data Subject has granted its Consent.

## **9.8. Right to Withdraw the Consent**

- 9.8.1. Where the Processing of Personal Data is performed based on the Consent, the Data Subject shall have the right to withdraw the Consent.
- 9.8.2. As a result of Consent withdrawal, the Bank will no further process Personal Data for the purposes according to which the Consent had been withdrawn, unless other legal basis for the Processing of Personal Data exists. After withdrawal of the Consent, the Bank shall have the right to process Personal Data for other legitimate purposes.

## **10. Cookies**

The Bank uses cookies on its websites. Additional information on the use of cookies is available at <https://www.ribbank.com/en/information-on-the-use-of-cookies>.

## **11. Video Surveillance**

- 11.1. To ensure the security of Bank's visitors, employees and property, video surveillance is carried out at the Bank.
- 11.2. The operation areas of video surveillance cameras are marked appropriately with an informative sign.

## **12. Exercising the Rights of the Data Subject**

- 12.1. The Data Subject has the right to request information regarding the processing of its data, as well as request deleting or modifying its data, if such data have changed or are inaccurate due to other reason, request restricting their processing, or object against the processing of its data. In such case, a written request shall be submitted (via Internet Banking or at the Bank's office). For the

purposes of requesting information, it is recommended using the Bank's form "Data Subject's Information Request" (IX.241) available at the Bank's home page.

- 12.2. The request shall precisely specify the specific Data Subject Categories by which the Data Subject is related to the Bank (potential customer, customer, potential employee, employee, or other category – if cooperation has taken place, but it cannot be included in other categories).
- 12.3. The Bank has the right to clarify the Data Subject's request, for example, by requesting specifying the period.
- 12.4. The Bank shall consider the Data Subject's request and carry out the said actions without undue delay, and in all cases, within 1 (one) month following the receipt of the request, inform the Data Subject about the actions carried out. The Bank may extend the request execution period for 2 (two) more months, taking into account the volume and complexity of the request. The Bank shall inform the Data Subject about the extension of the term and the reasons for the extension within 1 (one) month following the receipt of the request.
- 12.5. A reply to the request of the Data Subject may be provided to the Data Subject in one of the following ways:
  - 12.5.1. sent via Internet Banking if the Data Subject has access to Internet Banking and it is technically possible;
  - 12.5.2. issued in person in the Bank or the Bank's representative office;
  - 12.5.3. via other means of communication, where the Bank and the Data Subject have separately agreed thereon or the Data Subject has specified it in its request and the Bank, taking into account the sensitivity and volume of the information to be provided, considers that the specified means are suitable.

### **13. Special Provisions**

- 13.1. In cases stipulated in the normative acts binding for the Bank (for example, in cases stipulated in the AML/CFTP Law, etc.), the processing of Data, carried out by the Bank, shall not be subject to the Data Subject's right to request information regarding the processing of data, inter alia, its purposes, recipients, sources of retrieval; right to access its data and request their amendment, deletion, suspension or prohibition of processing. Hence, in cases stipulated in the normative acts, the Bank shall not provide any information to the Data Subject regarding the processing of Data, as well as not carry out any other actions requested by the Data Subject, which are prohibited by the binding normative acts.

### **14. Other Provisions**

- 14.1. Contact information of the Bank's Data Protection Specialist:  
datuaizsardziba@ribbank.com, or 2 J. Alunana St., Riga, LV-1010, marked "to the Data Protection Specialist".
- 14.2. If the Data Subject believes that the Bank has violated its rights in respect of Processing of Personal Data, the Data Subject shall be entitled to lodge a complaint with the personal data monitoring authority. A personal data monitoring authority in the Republic of Latvia is the Data State Inspectorate, address: 17 Elijas St., Riga, LV-1050.
- 14.3. The Bank shall have the right at any time unilaterally make amendments to the Data Processing Guidelines, informing the Data Subject thereof not later than 10 (ten) banking days in advance. The Bank shall inform the Data Subject about the amendments by placing information in the Bank premises and on the Bank's home page, or by sending information to the Data Subject electronically via Remote Communication Devices.