BluOr Bank

PRIVACY POLICY

www.bluorbank.lv

| Approved on 24.09.2025 | Valid as of 10.10.2025 | C2.2-1144/07 |

TABLE OF CONTENTS

BluOr Bank AS | Smilšu iela 6, Rīga, LV-1050, Latvija | Registration No. 40003551060 | SWIFT code: CBBRLV22
Phone: +371 67 031 333 | E-mail: info@bluorbank.lv | www.bluorbank.lv

TERMS AND ABBREVIATIONS

AML/CFT/CPF – anti-money laundering, combating the financing of terrorism and countering proliferation financing.

AML/CFT/CPF Law – Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing.

Applicant – Candidate or trainee.

Bank – BluOr Bank AS, registration No. 40003551060, address: Smilšu iela 6, Riga, Latvia, LV-1050, phone: +371 67 031 333, e-mail: info@bluorbank.lv, website: https://www.bluorbank.lv.

Candidate – a person who applies for a job in the Bank / Commercial Company of the Group.

Client – any natural person who uses, has used, or has expressed a wish to use any services provided by the Bank / Commercial Company of the Group or is in any other way connected with them (for example, the beneficial owner, authorised person, representative, guarantor, co-borrower etc.

Commercial Companies of the Group – commercial companies belonging to the Prudential Consolidation Group, except for the Bank – AS BBG, reg. No. 40003234829; AS Pils Pakalpojumi, reg. No. 40103170308; SIA BluOr International, reg. No. 40003444941; SIA ZapDvina Development, reg. No. 40003716809; SIA Jēkaba 2, reg. No. 40103293621; Kamaly Development UAB (reg. No. 300558022, Lithuania); Kamaly Developments EOOD (reg. No. 147093418, Bulgaria); Foxtran Management LTD (reg. No. 113.276, Belize); Thormano Limited (reg. No. HE 416193, Cyprus), HAZEE SHIPPING CORP (reg. No. 122754, Marshall Islands).

Controller – the Bank/Commercial Company of the Group that, alone or jointly with other Commercial Companies of the Group, determines the purposes and means of processing Personal Data.

Data Subject – an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier (such as a name, an identification number, location data, an online identifier etc.).

EEA – European Economic Area.

EU – European Union.

Personal Data – any information relating to the Data Subject.

Personal Data Breach – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

Policy – this "Privacy Policy".

Processing of Personal Data – any operation or set of operations which is performed on Personal Data or on sets of Personal 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.

Processor – a cooperation partner (a natural or legal person) which processes Personal Data on behalf of and in the interests of the Controller.

Prudential Consolidation Group (Group) – commercial companies included in the prudential consolidation group, which are determined on the basis of the criteria laid down in Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and amending Regulation (EU) No 648/2012, Credit Institution Law, the Bank of Latvia Regulation No. 266 "Regulations on the Exercise of Options Available in Directly Applicable EU Legislation on Prudential Requirements".

Recipient – Processor or Third Party.

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.

Third Party – a natural or legal person, public authority, agency or body other than the Data Subject, Controller, Processor and persons who, under the direct authority of the Controller or Processor, are authorised to process Personal Data.

1. GENERAL PROVISIONS

1.1. The purpose of the Privacy Policy is to protect the fundamental rights and freedoms of natural persons in relation to the processing of Personal Data by the Group in accordance with the applicable laws and regulations of the Republic of Latvia and the EU in the field of personal data protection, as well as to disclose information about the processing of Personal Data to the Data Subject in accordance with the requirements of the Regulation.

1.2. The Policy shall lay down the general procedures for the processing of Personal Data, defining the main purposes of Personal Data processing and the conditions for determining the legal basis, the applicable basic principles of Personal Data protection when processing Personal Data, as well as the storage period of Personal Data and the cases when Personal Data are transferred to Recipients and to third countries, and the procedures by which the Data Subject may exercise their rights.

1.3. The Policy has been developed taking into account the requirements of the Regulation, which are aimed at ensuring the security of Personal Data. The Group shall process the Personal Data of a natural person, respecting the interests of the person to protect their privacy.

1.4. Within the framework of applicable laws and regulations, the Group shall ensure the confidentiality of Personal Data and has implemented appropriate technical and organisational measures to protect Personal Data against unauthorized access, unlawful processing, disclosure, accidental loss, alteration or destruction.

1.5. Commercial Companies of the Group, taking into account their business models, can develop and approve their privacy policies and other internal regulatory documents that regulate in detail various issues related to the protection of personal data, observing the following principles:

1.5.1. such internal documents must comply with the principles established in the Policy, Regulation and other external regulatory enactments;

1.5.2. if a Commercial Company of the Group chooses not to develop a separate privacy policy, this Policy shall be binding on it to the fullest extent.

1.6. The Bank and Commercial Companies of the Group shall implement the Group-wide policy and procedures regarding the information exchange established within the Group for AML/CFT/CPF purposes.

1.7. In certain cases, when processing Personal Data, the Bank may act as a Processor on behalf of another controller, for example, as an insurance agent offering insurance services to its clients. In these cases, the Policy shall be applicable to the processing of the relevant Personal Data to the extent that it does not contradict the instructions provided by the relevant controller or its privacy policy.

1.8. When the Controller publishes various posts in the Bank's social network profiles (for example, various news about the Bank's professional activities, information on corporate internal, external events, achievements of the Bank's officials or employees, interviews, job advertisements etc.), publications may be accompanied by comments from individuals or marked by a person's reaction to a particular message. In these cases, the Policy shall not apply to the processing of the relevant Personal Data.

1.9. The terms used herein shall correspond to the terms used in the Regulation.

1.10. This Policy shall be binding to all employees and officials of the Bank/Commercial Companies of the Group.

1.11. The Bank's cookie policy is available on the Bank's website: https://www.bluorbank.lv/en/cookie-policy.

1.12. This Policy is drafted in Latvian and translated into English and Russian. In case of linguistic or interpretative disputes or disagreements, the text of the Policy in Latvian shall be legally binding.

2. GENERAL PRINCIPLES OF PERSONAL DATA PROCESSING

2.1. In order to ensure that the processing of Personal Data is secure and compliant with the requirements of the Regulation and other regulatory enactments, the Controller shall observe the following principles relating to processing of Personal Data:

2.1.1. Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject (**'lawfulness, fairness and transparency'**). In implementing this principle, the Bank has developed and is regularly updating this Policy, by which it informs the Data Subject of the processing of his/her Personal Data, thus ensuring that Personal Data are not used for any other purposes than those for which they have been collected. The Group shall respect the rights of the Data Subject by enabling him/her to control and monitor the processing of his/her data (see Section 11 herein);

2.1.2. Personal Data shall be processed for clear purposes and solely according to them (**'purpose limitation'**). The Group shall not collect and store Personal Data for unclear future purposes, the need for which has not been assessed and the commencement of implementation of which has not been approved by laws and regulations or internal regulatory documents;

BluOr Bank AS | Smilšu iela 6, Rīga, LV-1050, Latvija | Registration No. 40003551060 | SWIFT code: CBBRLV22
Phone: +371 67 031 333 | E-mail: info@bluorbank.lv | www.bluorbank.lv

2.1.3. Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**'data minimisation'**). In implementing this principle, the Group shall not request and process more information from the Data Subject than is necessary for attaining the relevant purpose;

2.1.4. Personal Data shall be accurate (**'accuracy'**). The Bank/Commercial Companies of the Group shall ensure correct and accurate processing of Personal Data. If the Bank/Commercial Company of the Group has any doubts about the relevance or correctness of the information provided by the Data Subject, the Bank/Commercial Company of the Group shall contact the Data Subject to clarify the information being processed. It is the duty of the Data Subject – the Client – to notify the Bank/Commercial Company of the Group if any information previously provided by them has changed (for example, person's surname, telephone number, residence address, etc.) has changed;

2.1.5. Personal Data shall be retained for no longer than is necessary (**'storage limitation'**). The Group shall process Personal Data for no longer than is necessary for achieving a specific purpose. An exception shall be, when upon the termination of a specific purpose another legitimate purpose occurs (see Section 12 herein);

2.1.6. Personal Data shall be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, by applying appropriate technical or organisational measures (**'integrity and confidentiality'**). The Group shall protect Client data using modern technologies, taking into account the existing privacy risks (for example, various security measures shall be used – data encryption when transmitting data; firewalls; hacker protection, etc.); likewise, the information technology system shall be constantly improved by the Bank with the aim to ensure the security of Personal Data. The Group shall ensure that access to Personal Data is granted only to the employees requiring such an access in order to fulfil their job duties. The Bank has developed a number of regulatory documents that regulate the procedure for granting the right of access to information in the Group, the procedure for working with Personal Data, with other confidential or secret information. For the purposes of minimising the risk of breach of Personal Data, the Group shall monitor the activities relating to the processing of Personal Data, register every incident affecting data security and take measures to prevent further threats to data.

2.2. The Bank/Commercial Company of the Group shall be liable for compliance with the principles referred to in sub-paragraphs of paragraph 2.1 herein and ensure their observance as follows:

2.2.1. Implementing and regularly updating this Policy and ensuring the Group's operations are in compliance with it;

2.2.2. Introducing appropriate technical and organisational means and measures (including the development of internal regulatory documents, the performance of internal data processing audits);

2.2.3. Carrying out regular training of existing and new employees on the processing and protection of Personal Data, as well as on compliance with confidentiality and ethical standards;

2.2.4. Updating internal regulatory documents with regard to processing activities;

2.2.5. Carrying out data protection impact assessment, if necessary;

2.2.6. Introducing and maintaining a Personal Data processing register, which records all information regarding Personal Data processing activities (the purpose of processing of Personal Data; legal basis; categories of data; categories of Data Subject; recipients of data; transfer of data to third countries; periods of storage; etc.);

2.2.7. Designating a data protection officer;

2.2.8. Preparing responses to the Data Subject regarding his/her rights and the processing of Personal Data by the Group.

2.3. If a Personal Data Breach results or is likely to result in a high threat to the rights and freedoms of the Data Subject, the Bank/Commercial Company of the Group shall inform the Data Subject and the Data State Inspectorate thereof in accordance with the requirements of the Regulation and the internal regulatory documents of the Bank.

2.4. Detailed information on the processing of Personal Data is further described in the agreements and other documents related to the services, as well as on the Bank's website.

3. DATA SUBJECTS AND COLLECTION OF PERSONAL DATA

3.1. Personal Data may be collected:

3.1.1. Directly from the Data Subject;

3.1.2. Based on Client service activities (such as cookies, IP addresses, authorization, on-line purchases etc.);

3.1.3. From external sources – public and private registers or Third Parties (e.g. from parties acquiring potential borrowers, borrowers – legal persons providing loans to individuals, etc.).

3.2. The Bank shall record telephone calls, visual images, video and/or audio files, save e-mail communication or otherwise document the Client's interaction and communication with the Bank, including collecting Personal Data during video and audio streaming, or during Client remote identification.

BluOr Bank AS | Smilšu iela 6, Rīga, LV-1050, Latvija | Registration No. 40003551060 | SWIFT code: CBBRLV22
Phone: +371 67 031 333 | E-mail: info@bluorbank.lv | www.bluorbank.lv

3.3. The Bank (in some cases, Commercial Companies of the Group) shall mainly process Personal Data of individuals who:

3.3.1. Apply for services;

3.3.2. Have entered or are willing to enter into an agreement, such as Clients;

3.3.3. Such persons as: legal agents, authorised persons, politically exposed persons, their family members or persons closely related to them, persons closely related to the officials or employees of the Bank/Commercial Companies of the Group, contact persons, business partners, payers, heirs, holders of the subject of insurance policy, applicants and visitors of the premises of the Bank/Commercial Companies of the Group;

3.3.4. Are related to Clients: additional users of safe deposit boxes, payment card users, or legal entities (e.g., shareholders (members), board members, company representatives, true beneficiaries, co-borrowers, guarantors, pledgers etc.).

4. CATEGORIES OF PERSONAL DATA

4.1. The categories of Personal Data that will be collected and processed primarily by the Bank (in some cases, Commercial Companies of the Group), but not only, are as follows:

4.1.1. **Identification data:** Data Subject's name and surname, username, personal ID number; taxpayer ID number;

4.1.2. **Authentication data:** personal signature, password assigned to the Data Subject, and other data required for the authentication of persons or users;

4.1.3. **Identity document data:** birth data, citizenship and other data specified in the identity document;

4.1.4. **Contact details:** actual and/or declared residence address; telephone number; e-mail address; language of communication;

4.1.5. **Family data:** marital status; information about the Data Subject's spouse or registered partner, dependants, heirs and other related persons;

4.1.6. **Data on professional activity:** level of education; work experience; skills and competencies;

4.1.7. **Client's financial data:** accounts; account statements at the Bank and other financial institutions; ownership; transactions; loans; income; liabilities; collateral and relevant data; credit history and creditworthiness; Client's financial experience and investment goals, including data collected during the selection and provision of investment services, insurance services, and other products related to the investment risk management; commercial requests or performed transactions with financial instruments;

4.1.8. **Data on the origin of funds or assets:** for example, information about the Client's counterparties and economic activities;

4.1.9. **Due diligence data on the Client and Client's related persons:** data on payment habits; tax residence; data that enable the Bank to carry out relating to the due diligence activities in the area of AML/CFT/CPF, and to validate the observance of national or international sanctions, including the goal of cooperation, and the status of the Client (a politically exposed person or US related person);

4.1.10. **Data on the eligibility of potential employees:** criminal records; information on insolvency; information on violations of laws and regulations governing international or national sanctions or AML/CFT/CPF;

4.1.11. **Data obtained and/or generated in fulfilling duties stipulated by laws and regulations:** data arising from requests of non-disclosable information received from public authorities, public officials or other authorities and officials; information regarding income, credit obligations, owned properties, notes and historic notes in databases, as well as remaining debt obligations etc.;

4.1.12. **Communication data:** data collected when the Data Subject visits the Client Service Centre of the Bank, the Internet Bank, and other places in which the Bank provides services, or contacts the Bank by phone; e-mail messages and other messages; data from social media; data obtained when the Data Subject visits Bank's websites or contacts the Bank through other communication channels of the Bank;

4.1.13. **Data related to services:** performance or non-performance of an agreement; performed transactions; use of ATMs; signed and invalid contracts; submitted applications, requests and complaints; service charges;

4.1.14. **Data on habits and satisfaction:** activity of using services; used services; personal settings; answers to survey questions; Client satisfaction assessment;

4.1.15. **Data on participation in lotteries and campaigns:** obtained points; prizes received in games or campaigns;

4.1.16. **Information necessary for making and processing payments:** Client's current account number with the Bank; payment card information; payment history; account statements; payment details, data on the payee/payer;

4.1.17. **Information on the user of Bank's website:** cookies, IP address;

4.1.18. **Visual appearance of a person:** video surveillance, screenshots with personal image, photos;

4.1.19. **Audio recordings:** business order approvals, technical details of the conversation (duration of the conversation, phone number of the call maker and the call recipient, time and date of the conversation);

4.1.20. **Complaint/whistleblower report data:** the conduct of the person, the results thereof, the details of the alleged or existing breach or deficiency;

BluOr Bank AS | Smilšu iela 6, Rīga, LV-1050, Latvija | Registration No. 40003551060 | SWIFT code: CBBRLV22
Phone: +371 67 031 333 | E-mail: info@bluorbank.lv | www.bluorbank.lv

4.1.21. **Data of requests submitted by Data Subjects:** details of the request, results, mutual correspondence data;

4.1.22. **Data on the risk of conflict of interest and the risk of corruption:** information regarding situations of conflict of interest, risk of corruption in connection with accepting gifts, benefits;

4.1.23. **Data for the prevention of payment fraud:** information on devices used and network data, connection parameters, and other data necessary for detecting and preventing fraud.

5. PURPOSE AND LEGAL BASIS FOR THE PROCESSING OF PERSONAL DATA

5.1. In its operations, the Group shall process various types of Personal Data, the scope and nature of which are different, taking into account the diverse purposes of the processing of Personal Data.

5.2. The Group shall not process information which is not required to achieve the defined legitimate purposes. Before starting the processing of Personal Data, the Group shall always evaluate and determine the purposes of the processing of Personal Data.

5.3. The Bank shall process Personal Data primarily for the following purposes:

5.3.1. To provide and administer financial services:

5.3.1.1. On-site and off-site identification and authentication of a Client prior to establishing a business relationship with the Bank;

5.3.1.2. Conducting Client due diligence;

5.3.1.3. Preparation and conclusion of agreements (e.g., account opening and maintenance agreements, loan agreements, credit card agreements) and fulfilment of contractual obligations;

5.3.1.4. Provision of remote services and authentication;

5.3.1.5. Assessment of creditworthiness, including evaluation of credit risk, ability to fulfil contractual obligations, and loan monitoring;

5.3.1.6. Provision of insurance services;

5.3.1.7. Account maintenance, provision of payment services, provision of payment initiation or account information services;

5.3.1.8. Fulfilment of duties established by laws and regulations (e.g., compliance with the requirements of the AML/CFT/CPF Law; notification of the Credit Register of the Bank of Latvia, AS "Kredītinformācijas Birojs", transfer of Personal Data to third-party payment service providers for the provision of account information and/or payment initiation services);

5.3.2. To provide one-time services to a Data Subject who is not a Client of the Bank (e.g., currency exchange);

5.3.3. To promote and distribute services, including marketing purposes, such as sending individual credit offers, advertising the Bank's services, conducting client surveys and research, organizing lotteries and prize draws, etc.;

5.3.4. To handle and process complaints;

5.3.5. To handle and process whistleblower alerts;

5.3.6. To protect its legitimate rights (e.g., debt recovery and collection);

5.3.7. To develop, maintain, and improve the Bank's services, internal processes, website, and mobile applications;

5.3.8. To disclose confidential information to public authorities, state officials, or other institutions and officials as required by applicable laws and regulations (e.g., to the State Revenue Service, courts, police, prosecutor's office, sworn bailiffs, notaries, insolvency administrators, etc.);

5.3.9. To ensure the security of the Bank and/or the Client, protect the life and health of the Client and/or their representatives, and safeguard other rights of the Bank and the Client (including visual and/or audio recordings), based on the Bank's legitimate interests;

5.3.10. To manage personnel;

5.3.11. To manage risks, including conflicts of interest and corruption risks, and to prevent payment fraud;

5.3.12. To fulfil obligations under international treaties and legal requirements in the field of taxation, obligations related to automatic exchange of financial account information, and other specified obligations.

BluOr Bank AS | Smilšu iela 6, Rīga, LV-1050, Latvija | Registration No. 40003551060 | SWIFT code: CBBRLV22
Phone: +371 67 031 333 | E-mail: info@bluorbank.lv | www.bluorbank.lv

5.4. Commercial Companies of the Group shall process Personal Data primarily for the following purposes:

5.4.1. To conduct Client due diligence;

5.4.2. To prepare and conclude an agreement and when fulfilling contractual obligations;

5.4.3. To assess creditworthiness, ability to fulfil obligations arising from the agreement, to supervise loans;

5.4.4. To fulfil obligations laid down in laws and regulations;

5.4.5. To protect their legitimate rights;

5.4.6. To manage personnel.

5.5. As a Controller, the Bank shall obtain Personal Data primarily by:

5.5.1. Identifying the Client and performing due diligence prior to establishing a business relationship;

5.5.2. Performing due diligence on the Client and monitoring payments during the business relationship;

5.5.3. Establishing contractual relationship with the Client and fulfilling contractual obligations (including, when requesting data from Third Parties);

5.5.4. Providing one-time services to a Data Subject who is not a Bank Client;

5.5.5. Consulting the Client by phone or receiving the Client's instructions for carrying out transactions by phone;

5.5.6. Requesting information about the Client from various registers;

5.5.7. Hiring new employees or engaging interns for practical training;

5.5.8. Receiving letters or e-mails from the Data Subject;

5.5.9. Conducting video surveillance in the Bank's premises, ATMs, or outside the Bank's premises;

5.5.10. Using information about the Data Subject from internet resources and other publicly available sources.

5.6. As Controllers, Commercial Companies of the Group shall obtain Personal Data primarily by:

5.6.1. Conducting due diligence on the Client during the business relationship;

5.6.2. Initiating contractual relationships and fulfilling contractual obligations;

5.6.3. Hiring new employees;

5.6.4. Receiving letters or emails from the Data Subject.

5.7. The Policy shall apply to the processing of Personal Data regardless of the form and/or environment in which the Client provides Personal Data (for example, on the Bank's website, in mobile applications, paper or telephone) and in which systems or hard copy they are processed.

5.8. The Group shall initiate the processing of Personal Data only if the processing of Personal Data has a specific purpose (for example, signing of an agreement; provision of a certain service; fulfilment of duties determined in laws and regulations etc.) and an appropriate legal basis.

5.9. If the Data Subject refuses to process Personal Data, the Bank/Commercial Company of the Group shall have grounds to refuse the provision of services of the Bank/Commercial Company of the Group.

5.10. Legal grounds for the processing of Personal Data may be the following:

	Legal basis	**Necessity**
5.10.1.	Establishment and fulfilment of contractual relationship	This legal basis shall ensure a possibility of processing Personal Data prior to entering into a contract in order to prepare the contract and process the Personal Data as long as the contract with the Data Subject is valid. With regard to the processing of Personal Data for the performance of a contract, the Data Subject shall have no right to prohibit the use of his/her data for the performance of the contract as long as the contract is valid. The Group shall request all the information necessary for entering into a contract; moreover, the legal basis shall apply also in cases where a contract is not signed due to any reason. The Bank shall apply this legal basis for the transfer of data to international card organisations (*Mastercard, VISA* etc.) to perform the agreement concluded between the Client and the Bank, as well as for the transfer of information to correspondent banks to enable the execution of payments in accordance with the payment account agreement, etc.

BluOr Bank AS | Smilšu iela 6, Rīga, LV-1050, Latvija | Registration No. 40003551060 | SWIFT code: CBBRLV22
Phone: +371 67 031 333 | E-mail: info@bluorbank.lv | www.bluorbank.lv

5.10.2.	Compliance with a legal obligation	The Group shall apply this legal basis to the processing of Personal Data, when the Group has no free choice of action – the relevant activity is regulated by the applicable laws and regulations of the EU or Latvia. For example, determining the status of the Client status or the suitability/compliance of investment services with Client interests, which is the Bank's obligation under the Financial Instruments Market Law. Also, the AML/CFT/CPF Law provides for a number of obligations imposed on the Bank, both in relation to the identification of the beneficial owner and a politically exposed person, and in relation to conducting the Client due diligence, etc.
5.10.3.	Protecting the vital interests of the Data Subject or of Third Parties	The Group shall apply this legal basis in exceptional cases, where the processing of Personal Data is carried out, for example, with the purpose of protecting the life or health of a person. For example, if the Data Subject incurs health problems in the premises of the Bank/Commercial Companies of the Group and the health condition must be discussed with the emergency medical assistance workers.
5.10.4.	Observance of the public interest or the exercise of official authority	Applies to cases where the Controller has official authority or carries out a task in the public interest and where processing is to be carried out in order to exercise such authority or to perform that task, as well as to situations where the Controller has no official authority but is required to disclose the data by a Third Party having such authority. Moreover, it may apply to situations where the Controller, upon request or on its own initiative, discloses data to a Third Party having such official authority. Such official authority or task in the public interest is usually stipulated by regulatory enactments. The Bank shall apply this legal basis for the processing of Personal Data, for example: 1) in accordance with Article 44 of the AML/CFT/CPF Law, which establishes the right of credit institutions and financial institutions to exchange information with each other; 2) when assessing its Clients' data using databases related to AML/CFT/CPF; 3) in order to achieve the objectives of the AML/CFT/CPF Law, as it is stipulated in Part One of Article 5(2) of the AML/CFT/CPF Law; 4) in accordance with the application of the Law on International Sanctions and National Sanctions of the Republic of Latvia in the context of the processing of Personal Data. However, in situations where there is no freedom of action due to a legal obligation, the Group shall process the data on the basis of sub-paragraph 5.10.2.
5.10.5.	Legitimate interests of the Group or Third Party	This legal basis shall be applied for ensuring the security of property (e.g., video surveillance, access control systems), monitoring service quality (e.g., recording of telephone calls), assessing creditworthiness during the credit granting and obligation monitoring process (including by using information from various external databases and automated account statement analysis), improving the Bank's financial services and processes, protecting its legitimate rights (e.g., debt recovery), preventing payment fraud, managing conflicts of interest and corruption risks, and for other similar purposes. When processing data based on this legal basis, the Group shall conduct a balancing of interests assessment prior to commencing the relevant processing. Upon the Data Subject's request, the Group may provide a summary of the results of the balancing of interests assessment.
5.10.6.	Consent given by the Data Subject	The Group shall apply this legal basis, for example, for marketing purposes, such as sending individual credit offers, when a person registers for lotteries or prize draws, or for receiving informational materials. The Data Subject shall have the freedom of choice – either to provide his/her consent to the processing of Personal Data or not; likewise, the Data Subject shall have the right to withdraw his/her consent at any time, thus discontinuing the processing concerned. The withdrawal of consent shall not affect the lawfulness of the processing of Personal Data, which has occurred before the receipt of withdrawal. For example, if the Bank sends the Client commercial notifications about existing or upcoming Bank services, or individual credit offers, based on the consent given by the Client, the Bank shall discontinue the further sending of information as soon as the Client has withdrawn his/her consent.

BluOr Bank AS | Smilšu iela 6, Rīga, LV-1050, Latvija | Registration No. 40003551060 | SWIFT code: CBBRLV22
Phone: +371 67 031 333 | E-mail: info@bluorbank.lv | www.bluorbank.lv

6. AUTOMATED INDIVIDUAL DECISION-MAKING, INCLUDING PROFILING

6.1. For services related to credit risk (e.g., payment cards with a credit limit, consumer loans), the Bank shall conduct automated individual decision-making during both the credit granting process and the monitoring of obligations, including profiling.

6.2. Profiling is automated processing of Personal Data that the Bank uses to analyse and evaluate the Client's credit risk. For profiling purposes, information provided by the Client to the Bank shall be used, including information on income, debts, marital status, number of dependents, etc., as well as information obtained from Third Parties (State Social Insurance Agency, State Revenue Service, AS "Kredītinformācijas Birojs", AS "CREFO Birojs", Credit Register of the Bank of Latvia, and, if the Client has consented, from debt recovery agencies) in accordance with the procedures and scope specified in the applicable regulatory enactments.

6.3. Based on the results of profiling, an automated individual decision shall be made determining:

6.3.1. Whether the Client is granted or denied a credit or credit limit;

6.3.2. If the credit or credit limit is granted – the amount and the applicable interest rate.

6.4. In the provision of deposit services to Clients identified remotely, the Bank shall make an automated individual decision with respect to parameters such as the maximum deposit amount, the Client's age, PEP status, connection to the United States, and age restrictions if the source of funds is 'pension or pension-like income', determining whether the service is approved or rejected.

6.5. For a credit risk-related service or a deposit service, automated individual decision-making shall ensure rapid, accurate and effective decision-making in concluding an agreement.

6.6. In meeting the requirements of the AML/CFT/CPF Law, the Bank shall employ a partially automated individual decision in respect of Client risk scoring that may potentially affect the application of Client surveillance measures. Such processing of Personal Data shall be carried out in the public interest, in meeting the requirements of the AML/CFT/CPF Law. Given that such data processing is carried out on the basis of laws and regulations, the exception referred to in point (b) of paragraph 2 of Article 22 of the Regulation shall apply, according to which such data processing is permitted and does not fall under the right of the Data Subject not to be subject to this decision.

6.7. A Client shall be entitled to express his or her opinion, as well as to challenge the automated individual decision made within the framework of a credit risk-related service or deposit service. In this case, the automated individual decision shall be reviewed by the Bank employee. The procedure for expressing an opinion or challenging the decision shall be laid down in paragraph 11.2.

6.8. The Bank shall review the request without undue delay and shall in any event respond within one month and inform of the actions taken.

7. PROCESSING OF APPLICANTS' PERSONAL DATA

7.1. Personal Data of Applicants may be obtained in one of the following ways:

7.1.1. From the Applicant submitting an application and CV (*Curriculum vitae*) to the Bank/Commercial Company of the Group to participate in the competition for a vacant position or internship;

7.1.2. If the Applicant has provided Personal Data for receiving feedback about them;

7.1.3. In the process of concluding a mutual contract with the Applicant;

7.1.4. From the Applicant, if any applications have been submitted, emails sent, or calls made;

7.1.5. Through websites *LinkedIn* or www.cv.lv.

7.2. The table below provides more information, indicating the purposes of processing the Applicant's Personal Data, categories, legal grounds for processing Personal Data and their storage periods.

Purpose of data processing	Personal data	Legal basis	Storage period
Evaluation of knowledge, skills, experience, recommendations for the vacancy for which the Applicant has applied, during the selection process	Name, surname, contact information, CV, application or motivation letters, recommendations, job interview questionnaires, certificates, interview results	Legitimate interests	1 year after the competition for a vacant position
Establishment of an employment relationship with the selected Candidate	Name, surname, ID number, contact information, salary, job title, information in the identity document, state language skills, residence permit (if necessary), information on the marriage certificate or other document confirming the change of surname, CV, job duties, term of contract, term of probationary period	Establishment and fulfilment of contractual relationship	90 years since the birth of a person

BluOr Bank AS | Smilšu iela 6, Rīga, LV-1050, Latvija | Registration No. 40003551060 | SWIFT code: CBBRLV22
Phone: +371 67 031 333 | E-mail: info@bluorbank.lv | www.bluorbank.lv

Internship agreements and additional agreements to internship agreements	Name, surname, information about the required internship program, educational institution, characteristics of the trainee, internship report, CV	Establishment and fulfilment of contractual relationship	10 years after expiry of the contract
Verification of Candidates' compliance with the requirements laid down in the Credit Institution Law	Name, surname, ID number, information on criminal record, insolvency, violation of laws and regulations governing international or national sanctions or AML/CFT/CPF	Legal obligation	30 calendar days
Retention of CVs of Applicants hired for employment or internship for compliance assessment purposes	Name, surname, contact information, CV	Legitimate interests	Until the Employee's or Intern's last working day

8. VIDEO SURVEILLANCE

8.1. Video surveillance shall be carried out inside and outside the premises of the Group. No audio recording shall be conducted during video surveillance.

8.2. Video surveillance shall not be carried out in areas with enhanced privacy (toilets, changing rooms, showers, etc.).

8.3. Processing of Personal Data shall be justified and necessary both for the legitimate interest of the Controller and for the benefit of Data Subjects.

8.4. Video surveillance shall also be carried out at the Bank's ATMs. Personal Data processed during video surveillance at the Bank's ATMs shall be included in visual images.

8.5. As part of video surveillance, the purpose of the processing of Personal Data shall be to prevent and identify criminal offences related to the protection of the property of the Controller and to protect vital interests of persons, including their life and health.

8.6. Information labels on video surveillance shall be placed in the areas of operation of surveillance cameras.

8.7. The information containing Personal Data – video and visual image recordings – shall be processed by the Processors, who, on behalf of the Bank, provide both physical security and cash handling services at the Bank's ATMs.

8.8. Video and visual image recordings obtained during the video surveillance may be transmitted to law enforcement authorities on request in accordance with the procedures specified in regulatory enactments, the content thereof may be disclosed and analysed within the scope of the relevant investigation.

9. TRANSFER OF PERSONAL DATA TO RECIPIENTS

9.1. In processing Personal Data, the Group's priority is to respect the confidentiality of information. The information may be transferred to the Recipients (see categories of Recipients of Personal Data in paragraph 9.2) to the extent and in the cases provided for by the applicable laws and regulations of Latvia and the EU, as well as for the purpose of ensuring the provision of high-quality services or when it is necessary for the performance of contractual obligations with the Data Subject.

9.2. The Bank/Commercial Company of the Group shall not disclose to the Recipient the Client's Personal Data or any information obtained during the provision of services and the performance of the agreement, including information about received financial services or other information, except for:

9.2.1. If the relevant Recipient has to transfer the data within the framework of the concluded agreement in order to perform a function necessary for the performance of the agreement (for example, payment initiation service) or delegated by a regulatory enactment;

9.2.2. If the Data Subject's explicit and unambiguous consent has been obtained;

9.2.3. If it is provided for by external laws and regulations and only in such case, to the extent and in accordance with the procedures laid down in laws and regulations (for example, law enforcement agencies, sworn bailiffs, sworn notary offices, tax administrations, supervisory authorities and financial investigation institutions);

9.2.4. If external laws and regulations impose certain obligations on the Bank;

9.2.5. Detecting fraudulent or malicious account use, preventing unauthorised use of payment instruments or payment-related fraud, and enabling the investigation and detection of such offenses;

9.2.6. In cases specified in external regulatory enactments for the protection of the Group's legitimate interests, for example, by applying to court or other state institutions against a Client who has infringed the legitimate interests of the Group, inter alia, to debt collectors according to the assigned right to claim; insolvency proceedings administrators;

BluOr Bank AS | Smilšu iela 6, Rīga, LV-1050, Latvija | Registration No. 40003551060 | SWIFT code: CBBRLV22
Phone: +371 67 031 333 | E-mail: info@bluorbank.lv | www.bluorbank.lv

9.2.7. To third parties specified in regulatory enactments, which maintain registers, for example, credit registers, registers of natural persons, commercial registers, securities registers, account registers, land registers and other registers, which contain or through which Personal Data are transferred;

9.2.8. To auditors, legal service providers, financial advisers or Processors of the Bank/Commercial Companies of the Group who carry out the processing of Personal Data on behalf of the Controller;

9.2.9. To credit institutions and financial institutions, providers of insurance services, third parties involved in the performance of transactions, making of payments and the reporting cycle, for example, places of execution (regulated markets, multilateral trading facilities and organised trading facilities), trade repositories, approved publishing structures, approved reporting systems, central counterparties, domestic and foreign brokers and depositories (The current list of correspondent banks of the Bank is available in the Bank's internet bank in the Section "Information" – Correspondent Banks; the list "Preferential Venues Used by BluOr Bank AS for Execution of Client Orders" is available on the Bank's website in the Section "Regulatory rules of bank's operation" – MiFID II);

9.2.10. To the related companies of the Bank;

9.2.11. To other persons who guarantee proper fulfilment of Client liabilities towards the Bank/Commercial Company of the Group, for example, warrantors, guarantee issuers, pledgers;

9.2.12. To participants in the European and International Settlement Systems, including SWIFT, and persons associated with them;

9.2.13. To the beneficial owners of the payment or transaction;

9.2.14. To insurance companies;

9.2.15. To Recipients related to the provision of services by the Bank/Commercial Companies of the Group, including providers of archiving, postal, telecommunication services;

9.2.16. To partners providing loyalty programmes and various privileges to Clients and employees of the Bank/Commercial Companies of the Group.

9.3. Prior to the transfer of data to the Processor, the Bank/Commercial Company of the Group shall enter into a contract with it, which details the procedure by which the Processor shall process and protect Personal Data, as well as ensure the deletion of Personal Data upon termination of the purpose of personal data processing within the framework of the performance of the contract.

9.4. Only the information necessary for the specified purpose shall be transferred to the Recipient.

9.5. Within the framework of the cooperation agreement or regulatory enactments, the Bank/Commercial Company of the Group shall ensure that the Recipient is notified of rectification, deletion or restriction of processing of Personal Data transferred to him in accordance with the Regulation, except where this is not possible or involves disproportionate effort. At the request of the Data Subject, in accordance with the procedure laid down in paragraph 11.2, the Bank/Commercial Company of the Group shall inform about the Recipients referred to in this paragraph.

9.6. If permitted by the nature of the processing, the Bank/Commercial Company of the Group may transfer pseudonymised information to the Recipient, by which the Recipient cannot identify the Data Subject concerned, or may use Personal Data encryption.

9.7. The Bank/Commercial Company of the Group may not enter into a contract with a Third Party only in cases where the transfer of the relevant data is regulated by the applicable laws and regulations of Latvia and the EU.

9.8. Recipients may process Personal Data both as Processors and as Third Parties. When the Recipient processes the Personal Data of the Data Subject on its own behalf as a Third Party, the Recipient shall be responsible for providing information about the processing of such Personal Data to the Data Subjects. In such case, the Group shall invite the Data Subject to contact this Recipient in order to obtain information about the processing of Personal Data by a Third Party (including the right of the Data Subject to erasure of Personal Data).

10. TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

10.1. In general, Personal Data shall be processed in the EU/EEA; however, in certain cases the data may be transferred to and processed in countries outside the EU/EEA (third countries). The transfer and processing of Personal Data outside the EU/EEA may occur if there is a legal basis for this, namely, to fulfil a legal obligation, to enter into or perform a contract, or in accordance with the Client's consent, and appropriate safeguards have been taken. Appropriate safeguards include, for example, a concluded agreement, including EU standard contractual clauses, which is approved under the Regulation; the Recipient is located in a country where, in accordance with the decision of the European Commission, an adequate level of protection of Personal Data is ensured; a decision is adopted by the European Commission on the adequate level of protection of Personal Data within the EU-US data privacy framework.

BluOr Bank AS | Smilšu iela 6, Rīga, LV-1050, Latvija | Registration No. 40003551060 | SWIFT code: CBBRLV22
Phone: +371 67 031 333 | E-mail: info@bluorbank.lv | www.bluorbank.lv

10.2. Payment service providers involved in the execution of financial services (including SWIFT payments) may be established or operate in a country that does not provide an adequate level of protection for Personal Data (i.e., in a country which has not acceded to the EEA Agreement and which has not been included by the European Commission in the list of countries ensuring an adequate level of protection of Personal Data). The Bank shall take the necessary measures to ensure that the transfer of Personal Data for the performance of financial services, the implementation of the objectives of the AML/CFT/CPF Law in accordance with the provisions of Article 44 of the AML/CFT/CPF Law, as well as ensuring compliance with other regulatory enactments, takes place in a secure manner. However, there is a risk that the Bank will not be able to ensure that the Recipient complies with the requirements of the Regulation in all cases. Therefore, before engaging in such transactions, the Bank invites to carefully evaluate the possible risks of processing Personal Data.

10.3. At the request, the Data Subject may receive more detailed information regarding the transfer of Personal Data to countries outside the EU / EEA.

11. RIGHTS OF THE DATA SUBJECT

11.1. The Data Subject shall have the right to obtain information regarding his/her Personal Data at the disposal of the Bank/Commercial Company of the Group, as well as to exercise the rights of the Data Subject laid down in the Regulation, by submitting a written request to the Bank/Commercial Company of the Group. This right of the Data Subject shall not apply to the processing of Personal Data, which is performed in order to fulfil the requirements of regulatory enactments regulating AML/CFT/CPF, as well as in other cases specified by regulatory enactments.

11.2. The Data Subject may submit requests for information addressed to the Bank (including about the rights of the Data Subject defined in the Regulation), complaints regarding the processing of his/her Personal Data or objections to the adoption of an automated individual decision in the following ways:

11.2.1. In writing, by submitting an application **in person** at the Client Service Centre (Jēkaba iela 2, Riga, LV-1050, Latvia), by presenting a personal identification document;

11.2.2. **Electronically**, by signing the application with a secure electronic signature and sending it by e-mail to datuaizsardziba@bluorbank.lv;

11.2.3. By sending a message in the **Internet Bank** of the Bank: https://ib.bluorbank.lv/.

11.3. The Data Subject may submit requests for information (including about the rights of the Data Subject defined in the Regulation) addressed to a Commercial Company of the Group and complaints regarding the processing of his/her Personal Data electronically, by signing the application with a secure electronic signature and sending it by e-mail to datuaizsardziba@bluorbank.lv.

11.4. Upon receiving a request of the Data Subject regarding the exercise of his/her right, the Bank shall validate the identity of the Data Subject. The information available to the Bank/Commercial Company of the Group regarding the Client and his/her transactions, which the Bank/Commercial Company of the Group obtains while providing financial services, in accordance with signed contracts, shall be treated as non-disclosable information in accordance with the Credit Institution Law and shall be presented only to the Client him-/herself or to his/her legal representatives.

11.5. The Group, in compliance with the requirements of the Regulation, has determined that:

11.5.1. Requests from the Data Subject addressed to the Processor shall be directed to the Bank/Commercial Company of the Group, which shall act as the Controller in accordance with paragraph 11.4;

11.5.2. Requests of the Data Subject, who has placed their deposit with the Bank through the deposit platform, regarding their Personal Data shall be received by the relevant deposit platform, which ensures the implementation of the requirements laid down in paragraph 11.4 and which transmits the request of the relevant Data Subject to the Bank for the exercise of the Data Subject's rights.

11.6. The Data Subject shall have the following rights with regard to the processing of their Personal Data:

11.6.1. **Receive information** regarding the processing of his/her Personal Data, purposes and legal grounds of processing, categories of Recipients, the data source if Personal Data is not collected from the Data Subject, the legal bases, the duration of storage or the criteria for establishing the storage term. If Personal Data has been collected from Third Parties and the acquisition and/or disclosure of such information is provided for in EU or Latvian laws and regulations, then in accordance with Article 14 Paragraph 5 of the Regulation, the Group shall have no obligation to inform the Data Subject about the processing of such Personal Data;

11.6.2. **Access** his/her data and receive confirmation of the processing of the data. For example, in the Bank's Internet Bank, the Client shall have the opportunity to get acquainted with information about account balances, Personal Data submitted to the Bank, payment history;

11.6.3. **Rectify** his/her data, if they are incorrect or inaccurate. The Data Subject shall, by submitting a reasoned request and information justifying it (if necessary), have the right to request the Bank/Commercial Company of the Group to supplement or rectify his/her Personal Data, which are inaccurate or incomplete, without undue delay;

11.6.4. **Erase** his/her Personal Data, i.e., the 'right to be forgotten', for example, if the data is no longer needed for the purposes for which it was collected, or if the Data Subject has withdrawn their consent on the basis of which the data was processed, if the Group has no other purpose and legal grounds for their further processing;

BluOr Bank AS | Smilšu iela 6, Rīga, LV-1050, Latvija | Registration No. 40003551060 | SWIFT code: CBBRLV22
Phone: +371 67 031 333 | E-mail: info@bluorbank.lv | www.bluorbank.lv

11.6.5. **Restrict** the processing of Personal Data, for example, if the Data Subject contests the accuracy of data, or if data are no longer necessary for the purposes set by the Group, but the Data Subject objects to the erasure of data for the establishment, exercise or defence of legal claims, etc.;

11.6.6. **Raise** objections against the processing of Personal Data, if the processing is in the legitimate interests of the Group or in the public interest. The right to object cannot be exercised if the legal basis for the processing of Personal Data is the consent given by the Data Subject, the establishment and fulfilment of contractual relationship, compliance with a legal obligation, protecting the vital interests of the Data Subject or of Third parties;

11.6.7. **Exercise the right to data portability** in order to retain the data or ensure repeated use of data, for example by transferring to another service provider. This right shall not be applicable to all the information. This right shall be applicable to the Personal Data provided by the Data Subject, for example, by filling out standard sheets and forms, applying for the use of Bank's products and services, as well as to the Personal Data processed by automated means (rather than using paper documents).

11.7. The Bank/Commercial Company of the Group shall examine the requests of the Data Subject without undue delay, but not later than within one month following the receipt of the request and provide a reply to the Data Subject informing about the measures to be taken in relation to his/her request. The Bank/Commercial Company of the Group may extend the deadline for the execution of requests for another two months, if there are grounds for this (for example, a large number of requests or complexity of requests).

11.8. The Bank/Commercial Company of the Group shall respond to the requests of the Data Subject, as well as perform any other activities related to the execution of the request of the Data Subject, free of charge, except in cases where the request is obviously unreasonable, excessive, or not commensurate with the resources at the disposal of the Bank/Commercial Company of the Group, namely, if the operation of the Bank/Commercial Company of the Group or the rights of other natural persons is/are threatened as a result of the execution of the request or the conditions for its execution.

11.9. The Data Subject shall have the right to submit a complaint if he/she considers that his/her Personal Data is processed in non-compliance with the requirements of laws and regulations: to the Data State Inspectorate, website: www.dvi.gov.lv, address: Elijas ielā 17, Riga, LV-1050, phone: 67223131, e-mail: pasts@dvi.gov.lv.

11.10. The Data Subject shall have the right to submit a complaint to the supervisory authority of the Member State in which his/her permanent place of residence, place of work or possible place of committing violation is located, if the Data Subject considers that the Bank/Commercial Company of the Group violates the requirements of laws and regulations in processing his/her Personal Data. Information on other supervisory authorities is available here: http://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm

12. STORAGE PERIOD OF PERSONAL DATA

12.1. Personal Data shall only be processed for as long as necessary. The storage period may be based on the Client agreement, Group's legitimate interests, or applicable laws and regulations (e.g., accounting regulations, AML/CFT/CPF requirements, the Civil Law in cases of limitation periods, etc.).

12.2. The Group shall store and process the Personal Data of the Data Subject as long as at least one of the following conditions exists:

12.2.1. Only as long as the contract with the Data Subject is in force;

12.2.2. As long as the Group or the Data Subject can exercise their legitimate interests in accordance with the procedures laid down in external laws and regulations (for example, to submit objections or bring an action in court);

12.2.3. While the Group has a legal obligation to store Personal Data;

12.2.4. As long as the Group has a reasonable basis for legitimate interests;

12.2.5. As long as the consent of the Data Subject to the relevant processing of Personal Data is in force, if there is no other legal basis for the processing of Personal Data.

12.3. After the expiry of the storage period of Personal Data in accordance with paragraph 12.2, Personal Data of the Data Subject shall be erased.

12.4. Personal Data processed in respect of the video surveillance conducted by the Bank (including at the Bank's ATMs) shall be stored for 1 or 3 months (depending on the area of operation of the surveillance cameras) from the moment of recording, unless another purpose of the processing arises (for example, requests from law enforcement authorities).

BluOr Bank AS | Smilšu iela 6, Rīga, LV-1050, Latvija | Registration No. 40003551060 | SWIFT code: CBBRLV22
Phone: +371 67 031 333 | E-mail: info@bluorbank.lv | www.bluorbank.lv

13. DATA PROTECTION OFFICER

13.1. The Data Protection Officer shall organise, control and supervise the compliance of the processing of Personal Data carried out by the Group as a Controller with the requirements of laws and regulations and this Policy, ensure cooperation with the supervisory authority – the Data State Inspectorate. The Data Protection Officer shall advise the employees of the Bank/Commercial Companies of the Group, who carry out the processing of Personal Data, on their duties in accordance with the Regulation and other regulatory enactments on data protection, as well as provide information to the Data Subjects, who address the Bank on issues related to the processing of Personal Data.

13.2. The Data Subject shall have the right to receive answers to general questions related to the processing of Personal Data within the Group (such questions shall not require the disclosure of confidential information). Requests for information regarding the processing of their Personal Data or complaints shall be submitted in accordance with the procedure specified in paragraph 11.2 of this Policy.

13.3. The Data Subject shall also have the right to withdraw the consent given for the processing of their Personal Data by submitting a request to the Bank in a free form via the Bank's Internet Bank or by writing to info@bluorbank.lv.

14. UPDATING OF THE POLICY

14.1. This Policy shall be updated in accordance with the changes in the processing of Personal Data by the Group and in accordance with amendments to external laws and regulations, but no less than once per year.

14.2. The data protection officer shall have the right to submit proposals to the Board of the Bank regarding improvement of the Personal Data protection system in the Bank/Group.

14.3. The Board of the Bank shall have the right to make amendments to the Policy and submit proposals for amendments to the Council of the Bank.

14.4. The Council of the Bank shall review the Policy at least once a year, assessing its relevance, and approve it.

14.5. The Policy with the amendments shall be published on the Bank's website, the message on the updating of the Policy shall be sent to the Clients of the Bank via the Internet Bank and deposit platforms (in cases where deposits with the Bank are placed via the platform), and shall be effective from the date of publication.

BluOr Bank AS | Smilšu iela 6, Rīga, LV-1050, Latvija | Registration No. 40003551060 | SWIFT code: CBBRLV22
Phone: +371 67 031 333 | E-mail: info@bluorbank.lv | www.bluorbank.lv