Terms and Conditions of Credit Card Agreement

BluOr Bank

BluOr Bank

CONTENTS

1. General Section . . . 1
2. Key Terms and Conditions . . . 4
3. Card Issuance and Renewal . . . 5
4. Use of the Card . . . 6
5. Use of Click to Pay . . . 8
6. Linking the Card to a Digital Wallet . . . 10
7. Keeping the Card Safe . . . 11
8. Loss of the Card . . . 11
9. Suspension of the Card . . . 11
10. Fees for Services . . . 12
11. Currency Conversion . . . 12
12. Insurance . . . 13
13. Investigation of Transactions . . . 13
14. Liability . . . 14
15. Changes to the Agreement . . . 16
16. Term and Termination of the Agreement . . . 16
17. Dispute Resolution . . . 18
18. Final Provisions . . . 19

1. GENERAL SECTION

1.1. The following terms are used in these Terms and Conditions:

Account – the Client's account with the Bank to which the Card is linked for making Card Transactions. This account is used to manage the credit card.

Account Statement – a document prepared by the Bank in paper or electronic form and provided to the Client. It shows all movements of funds in the Account during a specified period, as well as the Account balance at the beginning and end of that period.

Agreement – the agreement between the Client and the Bank, consisting of the Application, the Pricelist and these Terms and Conditions.

Application – a document prepared by the Bank that the Client completes and signs to apply for an account, a Card or other Bank services. The Client can sign the Application by hand or electronically. An Application completed and signed with an Electronic Signature has the same legal effect as a document signed by hand. Such a document can be used to resolve disputes between the Bank and the Client.

ATM – an electronic device used to deposit and/or withdraw cash with a Card and access certain other services offered by the Bank.

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

Authentication Methods – physical or digital methods involving various elements and data that the Bank accepts and uses to verify the Client's identity and confirm that the Client has authorised Transactions. These include:

- electronic identification methods and electronic signatures, such as Smart-ID, ID card, eParaksts Mobile and Mobile ID;
- the Digipass calculator issued by the Bank;
- PINs, passwords, the identification number assigned to the Client, personal identity number and other confidential information;
- the Client's biometric data, such as facial recognition or fingerprints (e.g. Touch ID, Face ID, Fingerprint);
- physical devices, such as mobile devices, smartwatches and other smart devices used to authenticate the Client;
- other authentication methods accepted by the Bank.

Bank – BluOr Bank AS.

Card – a credit card issued by the Bank and linked to the Account. A Card issued in the name of another person chosen by the Client is also referred to as a Supplementary Card in these Terms and Conditions.

Cardholder – the person in whose name the Card is issued. The Cardholder may be the Client or another person chosen by the Client.

Click to Pay – an online payment solution provided by an international card scheme. It allows the Cardholder to pay with their Card at merchants that offer Click to Pay without having to enter all their Card details each time.

Click to Pay Profile – information associated with the Cardholder and used to provide the Click to Pay service. This includes details of the Cards added to Click to Pay and the Cardholder's contact information.

Client – an individual, legal entity or legal arrangement that has entered into this Agreement and whose Account is linked to the Card.

Commission Fee or Commission – a fee charged by the Bank for its services, as specified in the Pricelist.

Consent – the Client's consent (authorisation) to carry out a Transaction. Unless otherwise stated in the Agreement, the methods and forms of giving Consent are set out in this Agreement and the GTB.

Consumer – a Client who is an individual and uses the Bank's services (makes Transactions) for purposes unrelated to their business or professional activities.

Credit Limit – an amount of money that the Bank allows the Client to use in addition to the funds available in the Account.

CVV2 Code – the three-digit security code on the back of the Card used for online purchases.

Digital Card – a digital version of a Card issued by the Bank.

Electronic Signature – codes, passwords or other actions that the Client creates, uses or takes using an Authentication Method. These allow the Bank to identify the

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

Client in the Internet Bank or other Bank systems. An Electronic Signature links the Client to a specific document, such as an Application, questionnaire or agreement, or to a Transaction or Order. The Bank treats an Electronic Signature as the Client's Consent. It is used in accordance with the terms of the Agreement. An Electronic Signature also includes a secure electronic signature that complies with Laws and Regulations.

Exchange Rate – the currency exchange rate used when the currency of a Transaction differs from the currency of the Card.

GTB – the Bank's General Terms of Business.

Interest – a fee charged for an Unauthorised Credit Limit, payable in accordance with these Terms and Conditions and at the interest rate specified in the Pricelist.

International Card Organisation – Mastercard, Visa or any other payment card organisation whose payment system is used to process Transactions.

Internet Bank – the Bank's remote banking service.

The Client can use the Internet Bank to:

- access their banking services;
- communicate with the Bank.

The Internet Bank can be accessed:

- through the Bank's website at http://www.bluorbank.lv;
- through the Bank's Mobile App.

Laws and Regulations – the laws and regulations of the Republic of Latvia, rules issued by competent authorities, other legal requirements governing the relationship between the Bank and the Client, the rules of the International Card Organisation, and good banking practice. Foreign laws and regulations apply if required by the laws and regulations of the Republic of Latvia or the Agreement.

Merchant – a person or business that accepts Cards as payment for goods and services, including payments made through websites and online platforms.

Mobile App – the Bank's Blue KEY mobile app, which the Client can use to log in to the Internet Bank, approve payments and Transactions, and sign messages to the Bank in the Internet Bank. The Mobile App is designed specifically for mobile devices and can be downloaded from app stores such as the Apple App Store (iOS) and Google Play Store (Android).

Parties – the Bank and the Client together. Each is individually referred to as a Party.

PIN Code – a combination of numbers known only to the Cardholder, provided digitally by the Bank through the Internet Bank and Mobile App. The Cardholder uses the PIN Code as their signature (Consent) to authorise certain Transactions and access the Bank's services available at ATMs.

Pricelist – a document setting out the fees charged for the Bank's services. The Pricelist is available on the Bank's website, in the Internet Bank and/or at the Client Service Centre.

Reserved Amount – money that has not yet been debited from the Account after the Client makes a Transaction or performs another operation on their Account because

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

the Bank is still processing it. The money may be reserved for up to 30 calendar days, starting from the date the Client makes the Transaction or performs the operation on their Account.

Settlement Period – a period of one calendar month that ends on the last Bank business day of the month. The first Settlement Period begins on the day the first Transaction is posted to the Account and ends on the last Bank business day of that month.

Token – a unique digital identifier that replaces the Card number and is used to make and process Transactions through Click to Pay.

Transaction – a cash deposit, cash withdrawal, purchase, transfer of funds or any other transaction that creates an obligation using the Card. This includes any action that increases or decreases the Account balance, as well as any other action authorised by the Cardholder using the Card.

Transaction Limits – limits set by the Client or the Bank on Transactions based on their type, amount, number and time period.

Unauthorised Credit Limit – a negative balance in the Account.

Unauthorised Transaction – a Transaction to which the Client has not given their Consent.

2. KEY TERMS AND CONDITIONS

2.1. The Bank will issue a Card to the Cardholder and allow the Cardholder to make Transactions using the Card, subject to the applicable Transaction Limits, the funds available in the Account and any Credit Limit granted.

2.2. The Card remains the property of the Bank and is issued to a specific Cardholder whose first name and surname appear on the Card. Only this person is allowed to use the Card.

2.3. The Client must use the Card in accordance with the Agreement.

2.4. The Client must pay for the services they receive in accordance with the Pricelist and the Agreement.

2.5. The Agreement governs the relationship between the Bank and the Client concerning the issuance, use and servicing of the Card. If the Client wishes to obtain a Credit Limit, a separate agreement must be concluded.

2.6. Any matters concerning the relationship between the Bank and the Client that are not covered by this Agreement are governed by the GTB and Laws and Regulations.

2.7. To make purchases online, the Client must enable the relevant feature. This feature can be enabled or disabled in the Internet Bank or Mobile App.

2.8. The Cardholder can use both a plastic Card and its digital version available on their mobile device. The Bank may allow the Cardholder to use the Digital Card before receiving and activating the plastic Card. The Client should note that the plastic Card and Digital Card may have different features, depending on the Bank's technical capabilities.

2.9. The Client must not disclose Card details, including the Card number, PIN Code and CVV2 Code, or any other information about the Agreement, the Client, the Card or

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

other documents related to the Agreement to anyone else. Such information may only be disclosed if necessary to make Transactions or register the Card for future Transactions.

2.10. The rules for using the Card and PIN Code are set out in the Agreement, the Account Opening and Servicing Agreement, the GTB and Laws and Regulations.

2.11. The Card's expiry date is shown on the Card as a month and year.

2.12. The Card is valid until the last day of the month shown.

3. CARD ISSUANCE AND RENEWAL

3.1. The Client can collect the Card from the Bank. To start using the Card, the Client must activate it in the Internet Bank or Mobile App.

3.2. The Card can also be sent by post or courier to an address provided by the Client. To start using the Card, the Client must activate it in the Internet Bank or Mobile App.

3.3. If the Card is sent by post or courier, the Client assumes the risks associated with its delivery.

3.4. The Client must inform the Bank if:

- the Card sent by the Bank has not arrived;
- the Card or its packaging is damaged;
- there are other reasons why the Client cannot receive the Card.

3.5. The Client may designate several Cardholders for their Account.

3.6. When the Card expires, the Bank will produce and issue a new Card with a new expiry date. This does not apply in the cases specified in Clause 16.4 of the Agreement.

3.7. The Client can collect the renewed Card from the Bank, have it delivered to an address provided by the Client through a postal service provider, or receive it in another way agreed by the Parties.

3.8. The Bank provides the PIN Code digitally through the Internet Bank or Mobile App.

3.9. When the Card is renewed, the PIN Code is changed.

3.10. The PIN Code is confidential and must only be used by the Cardholder.

3.11. To activate contactless payments, the Client must make the first Transaction by inserting the Card into a payment terminal or ATM and entering the PIN Code.

3.12. For security reasons, the Bank may cancel or destroy the Card and terminate the Agreement if:

- the Card has been issued or sent to the Client but has not been activated within three months of its issuance or dispatch;
- the Card has been produced but the Client has not collected it from the Bank within three months of its production.

3.13. If the Card is destroyed or cancelled, or if the Client refuses to collect the ordered Card or does not activate it, the Client must still pay the applicable fees for Account maintenance, Card replacement and delivery until the Bank receives an Application to close the Account.

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. USE OF THE CARD

4.1. The Card is a plastic card with a magnetic stripe, a chip and a contactless antenna.

4.2. The Cardholder may only use the Card to make Transactions.

4.3. The Card can be used to make Transactions wherever the Bank or another party provides Card acceptance services.

4.4. Funds in the Account are used to pay for Card Transactions. The Client must ensure that there are sufficient funds in the Account to make Transactions.

4.5. If the Cardholder makes a Transaction and there are insufficient funds in the Account to cover it, the Client must immediately repay the overdrawn amount to the Bank by depositing the required funds into their Account.

4.6. The Client may change the Transaction Limits through the Internet Bank or Mobile App, or by submitting a written request to the Bank.

4.7. A Card Transaction is considered authorised if the Cardholder has given their Consent. Depending on how the Card is used, Consent to a Transaction may be given by:

- entering the PIN Code when the Card is inserted into a payment terminal or ATM, or when the Bank requires the PIN Code to authorise a contactless Transaction;
- holding the Card or a device containing the Digital Card close to a payment terminal or ATM so that the Card details can be read when using the contactless feature;
- using the Card with an additional security system (3-D Secure). In this case, the Merchant will ask the Cardholder to enter a code from their Internet Bank authorisation tool, in addition to the Card number and expiry date;
- using a contactless Card, either on its own or together with the PIN Code;
- entering the Card and Cardholder details in an online store, whether or not the Merchant requires an additional security system;
- making Transactions using a Digital Wallet linked to the Card. For in-person Transactions, the Cardholder must hold the device containing the Digital Wallet close to a payment terminal, with or without additional confirmation, if this is supported by the Digital Wallet provider and accepted by the Bank;
- using the Card and a signature, where applicable.

4.8. Once a Transaction has been authorised as described in Clause 4.7, it cannot be revoked.

4.9. If the Cardholder believes that a Transaction was unauthorised or incorrect, they must inform the Bank in writing, either in person or through the Internet Bank, immediately and no later than 60 days after the Transaction was executed, if:

- an Unauthorised Transaction has been made;
- a Transaction has been processed incorrectly;
- an incorrect Transaction amount has been debited from the Account;

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

- there are errors in the Commission Fees calculated by the Bank.

The Cardholder must provide the Bank with all requested information and documents, including any evidence needed to review and, if necessary, investigate the disputed Transaction.

4.10. The release of a Reserved Amount does not affect the authorisation of the Transaction. The Client must ensure that there are sufficient funds in the Account to complete the Transaction unless the Merchant has cancelled it.

4.11. The Cardholder must not use the Card to make Transactions or perform any other activities prohibited by Laws and Regulations or the Agreement.

4.12. When making a Transaction at a Merchant, the Client must show an identity document if requested by the Merchant's employee.

4.13. The Cardholder must ensure that Card Transactions are carried out in their presence.

4.14. The Cardholder must check that the Transaction amount is correct. They must not authorise a Transaction if the amount is missing or incorrect.

4.15. If the Cardholder enters an incorrect PIN Code three times in a row at an ATM, the ATM may retain the Card. In this case, the Card must be replaced with a new one.

4.16. If the Cardholder enters an incorrect PIN Code three times in a row at a Merchant's PIN entry device, the Card will be automatically blocked. The Cardholder can unblock the Card at an ATM by entering the correct PIN Code.

4.17. The Cardholder must not use the Card after its expiry date. An expired Card must be destroyed.

4.18. The Cardholder must not take any action that involves converting any Card details (such as the Card number or CVV2 Code) into electronic form and sending, uploading or entering them into an information system, unless this is directly necessary to make Transactions. This restriction does not apply to the transfer or processing of Card details through a payment solution approved by the Bank, including Click to Pay, to the extent necessary to use the relevant service.

4.19. If the Card provides access to the Priority Pass programme, the Client must read the Priority Pass Terms and Conditions before using its benefits and services.

4.20. The Priority Pass Terms and Conditions are available at www.prioritypass.com. The Client must accept and comply with them. The following conditions apply to the Priority Pass programme:

- Priority Pass members can access the benefits and services offered under the programme (www.prioritypass.com);
- Fees for Priority Pass services are debited from the Account linked to the Card that provides access to the Priority Pass programme. If there are insufficient funds in the Account, the service will not be provided;
- The Client is fully responsible for the Priority Pass services they receive. The Client must cover any losses the Bank incurs or may incur as a result of these services. The Bank is not liable for any losses suffered by the Client in such cases;

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

- The Bank does not accept or investigate complaints about Priority Pass services, their terms and conditions, quality or fees charged;
- The Bank may terminate the Priority Pass service unilaterally if:
  - the Account linked to the Card that provides access to the Priority Pass programme is closed, or the Agreement for that Card is terminated;
  - the Bank stops offering the Priority Pass service.

5. USE OF CLICK TO PAY

5.1. The Bank may offer Click to Pay as a Card feature. Click to Pay allows the Cardholder to make online Transactions more easily with Merchants that offer Click to Pay.

5.2. The Bank may activate Click to Pay for a Card at the Cardholder's request, provided that the Card meets the requirements set by the International Card Organisation for using Click to Pay.

5.3. The Client can activate Click to Pay for the Card through the Mobile App.

5.4. Activating Click to Pay does not change the Card's basic features. The Cardholder can continue to use the Card in other ways permitted under the Agreement.

5.5. All terms of this Agreement that apply to Card Transactions also apply to Transactions made using Click to Pay.

5.6. To provide Click to Pay, the Bank may create a Click to Pay Profile and assign one or more Tokens to the Card if:

- the Bank has the Cardholder information needed to provide Click to Pay;
- the Cardholder has not opted out of Click to Pay.

5.7. The Bank uses the Cardholder's contact details, including their email address and mobile phone number, to create, maintain and update the Click to Pay Profile.

5.8. The Bank manages its relationship with the Cardholder in connection with Click to Pay. This includes providing information about the service and taking the necessary steps to update the Card and Click to Pay Profile details.

5.9. The Cardholder can manage their Click to Pay Profile in the dedicated Click to Pay section for the Card in the Mobile App.

5.10. The Cardholder is responsible for the contact details provided in their Click to Pay Profile and for keeping them up to date. The Bank is responsible for providing the Click to Pay Profile data to the International Card Organisation.

5.11. The technical solution for Click to Pay is provided by the International Card Organisation, but the organisation is not a party to the agreement between the Cardholder and the Merchant for the purchase of goods or services. Any issues concerning the quality, delivery, cancellation or refund of purchased goods or services must first be addressed with the Merchant. This clause does not limit the Cardholder's rights against the Bank under the Agreement or Laws and Regulations.

5.12. To provide Click to Pay, the Bank and the International Card Organisation may use and share information necessary for the service to work. This may include the

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

Cardholder's name, contact details, Card information and Click to Pay Profile details. More information about the processing of personal data is available on the Bank's website under "VISA payment cards for individuals" and in the Bank's Privacy Policy.

5.13. The Cardholder must ensure that the contact details provided to the Bank, including their mobile phone number and email address, are correct and up to date.

5.14. The Cardholder must inform the Bank immediately of any changes to the information used to provide Click to Pay.

5.15. The Cardholder must not share the Authentication Methods used to authorise Click to Pay Transactions with third parties.

5.16. The Cardholder must not use Click to Pay for illegal or fraudulent purposes, attempt to disrupt its operation, bypass security measures or access Click to Pay systems, software or data without authorisation.

5.17. The Cardholder must not copy, modify, decompile, disassemble or otherwise attempt to obtain the source code of the Click to Pay software, except where expressly permitted by Laws and Regulations.

5.18. The Bank may suspend or terminate access to Click to Pay entirely or for a specific Card if:

- the Card is blocked, cancelled or has expired;
- the Card no longer meets the International Card Organisation's requirements for using Click to Pay;
- there are reasonable grounds to suspect fraud, unauthorised use or a security threat;
- this is required by the International Card Organisation, the Bank's supervisory authority or Laws and Regulations.

5.19. The Cardholder can opt out of Click to Pay at any time using a method offered by the Bank. Opting out of Click to Pay does not terminate the Agreement, cancel the Card or restrict the use of the Card in other ways permitted under the Agreement.

5.20. If the Cardholder opts out of Click to Pay, the Bank will take the necessary steps to deactivate the Card for Click to Pay within a reasonable time. Certain data may be retained after deactivation if necessary to comply with Laws and Regulations, resolve disputes, ensure security or for other purposes specified in the Bank's Privacy Policy.

5.21. The Bank is not liable for Click to Pay being unavailable or not working properly due to circumstances beyond the Bank's control. These include technical problems with the systems of the International Card Organisation, Merchants, communication networks, the Cardholder's device or other third parties. This clause does not limit the Bank's liability where it cannot be excluded under Laws and Regulations.

5.22. The Bank will make changes to these Click to Pay Terms and Conditions in accordance with the procedure set out in Section 15 of the Agreement if the changes constitute amendments to the Agreement. The Bank may introduce technical or functional changes that do not affect the contractual rights or obligations of the Client or Cardholder without amending the Agreement.

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. LINKING THE CARD TO A DIGITAL WALLET

6.1. A Digital Wallet is a service that allows the Client to create a digital version of their Bank-issued Card on their mobile device and use it to make Transactions.

6.2. The Card can also be linked to Merchants' online platforms, such as subscription services, online stores, transport service providers and other services. The Cardholder must comply with the terms and conditions of the Merchant services to which they have linked their Card. This also applies to the payment terms for goods and services, such as subscription fees agreed between the Cardholder and the Merchant.

6.3. By adding the Card to a Digital Wallet of their choice, such as Apple Pay or Google Pay, and linking it to a mobile device on which the Digital Wallet is activated, the Client confirms that they have read and accepted these Terms and Conditions, the GTB, the Privacy Policy and the Pricelist, under which:

- The Client may only use the Digital Wallet on a mobile device that is accessible only to them and/or protected against accidental or intentional use by third parties (for example, by a PIN Code, biometric authentication or other security measures known only to the Client);
- The Client is solely responsible for keeping their Digital Wallet information confidential and their mobile device secure, including protecting login details, access codes and PIN Codes. The Client is also responsible for any losses resulting from using the Digital Wallet on a damaged, modified or otherwise compromised mobile device;
- The Client can use the Digital Wallet to make Transactions with the Digital Card in accordance with the Digital Wallet provider's terms and conditions, which the Client must read and accept. The Bank does not provide Digital Wallet services and is therefore not responsible for how the Digital Wallet operates;
- By holding a mobile device linked to the Digital Card close to a payment terminal and/or taking any other steps required by the Digital Wallet provider to authorise a Transaction, the Client gives their Consent to that Transaction;
- The Client must inform the Bank if:
  - a mobile device linked to the Digital Card is lost, stolen or otherwise unlawfully taken;
  - the Client's Digital Card is used without their Consent;
  - the Client believes that someone else knows the login details, access codes or PIN Codes for their mobile device or Digital Wallet.

6.4. The Client must remove the Card from the Digital Wallet on any mobile device they no longer intend to use and/or that may be used by another person.

6.5. Transaction data, which may include the Client's personal data, may be stored on the mobile device and shared with the Digital Wallet provider if necessary to process the relevant Transaction. This data will be processed in accordance with the Digital Wallet provider's Privacy Policy.

6.6. The Client's Card limits also apply to Transactions made using the Digital Wallet.

6.7. The Digital Card remains valid for payments until:

- the Cardholder removes or blocks the Card linked to the Digital Wallet;
- the Card is closed.

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

7. KEEPING THE CARD SAFE

7.1. The Cardholder must keep the Card and any mobile device containing the Digital Card secure to prevent other people from accessing them.

7.2. The Cardholder must not share the Card, Card number or other Card information with anyone unless this is directly necessary to make a Transaction.

7.3. The Cardholder must not disclose the PIN Code or any other information about the Client, the Agreement, the Card or other related documents.

7.4. The Cardholder must not keep the PIN Code together with the Card. Failure to comply with this requirement is considered gross negligence on the part of the Cardholder.

7.5. The Cardholder must protect the Card and any mobile devices containing the Digital Card from high temperatures, electromagnetic fields and physical damage.

8. LOSS OF THE CARD

8.1. If the Card or a mobile device containing the Digital Card is stolen, lost or otherwise falls into someone else's hands, or if the Card is retained by an ATM, the Cardholder must immediately block the Card through the Internet Bank.

8.2. The Cardholder must also do this if they suspect that someone else has obtained the PIN Code or other Card-related information. The Client can report this to the Bank during its business hours by calling +371 67 031 333 or, outside the Bank's business hours, by calling the 24-hour helpline of Nets Estonia AS, the company providing Card services, on +372 67 114 44 (service available in English).

8.3. The Cardholder must submit a written confirmation of the loss to the Bank, in any format, within seven days of reporting it verbally.

8.4. The confirmation can also be submitted through the Internet Bank or Mobile App using an Authentication Method.

8.5. The Cardholder must inform the Bank immediately if they find a Card that was previously reported as stolen or lost.

8.6. The Cardholder must not reactivate the Card through the Internet Bank if there is a possibility that someone else has obtained the Card's PIN Code or other Card details.

8.7. The Client is responsible for reactivating a previously blocked Card and for any Transactions made with the Card after its reactivation.

9. SUSPENSION OF THE CARD

9.1. The Bank will suspend the Card at the Cardholder's request.

9.2. The Bank may suspend the Card if the Client has spent more money than is available in the Account, resulting in an Unauthorised Credit Limit.

9.3. The Bank may require the Client to repay the debt within 30 days of receiving the Bank's notice.

9.4. Once the Client has repaid the debt, the Bank may reactivate the Card, provided that the Bank has not terminated the Agreement after the debt was repaid.

9.5. The Bank may also suspend the Card if the Client breaches other terms of the Agreement.

9.6. The Bank may also suspend the Card if it detects unusual Card Transactions.

9.7. The Card may also be suspended at the request of government authorities or officials, or in other cases specified by Laws and Regulations.

9.8. At the Client's request, the Bank will take the necessary steps to prevent a Supplementary Cardholder from making Card Transactions.

10. FEES FOR SERVICES

10.1. The Client must pay Commission Fees and other charges for the Bank's services in accordance with the Pricelist and the Agreement. This includes fees for issuing, replacing and renewing Cards, as well as for Transactions. The Bank may deduct these payments from any of the Client's accounts with the Bank.

10.2. To collect payments under the Agreement and the Pricelist, the Bank may calculate and deduct the following amounts from the Account or any other account held by the Client with the Bank, in the order listed below, without further approval from the Client:

- Account maintenance fee. This fee applies from the month the Account is opened and is charged for the current month;
- Commission Fees for Card Transactions, charged after the Transaction is made;
- Interest on an Unauthorised Credit Limit;
- other payments due from the Client under the Agreement and the Pricelist.

10.3. The Bank deducts payments as described in Clause 10.2. If necessary, the Bank may convert currencies using the exchange rate approved by the Bank on the settlement date.

10.4. The Bank deducts payments as described in Clause 10.2. If there are insufficient funds in the Account to cover Commission Fees and other payments, the Bank may create a negative balance in the Account.

10.5. The Bank provides a report in the Internet Bank showing the Transactions made, the Credit Limit used (if granted) and the amounts repaid.

10.6. The Client must ensure that sufficient funds are available in the Account. The Client must deposit enough money to cover the payments listed in Clause 10.2 and any contractual penalties, if applicable. The Client must do this no later than the end of the Settlement Period, unless an earlier payment due date applies.

11. CURRENCY CONVERSION

11.1. If the Transaction currency is not euro, the Transaction will be converted into euro using the exchange rates set by the International Card Organisations. Information about these exchange rates is available on the International Card Organisations' websites: https://www.visa.com.my/support/consumer/travel-support/exchange-rate-calculator.html.

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

11.2. If the Account currency differs from the Transaction currency, a currency conversion fee applies. This fee is specified in the Pricelist.

11.3. If the Cardholder makes a Card Transaction in a currency other than the Account currency, the Bank will, where required by Laws and Regulations, send the Cardholder information electronically about the currency conversion charges applied by the Bank. These charges are expressed as a percentage mark-up over the latest available euro foreign exchange reference rate issued by the European Central Bank. The Bank sends this information by SMS. The Cardholder can opt out of receiving these notifications through the Internet Bank, by calling the Bank during its business hours on +371 67 031 333, or by visiting a Client Service Centre.

11.4. By authorising a Transaction, the Client accepts the Exchange Rates applied by the Bank and the International Card Organisations. These rates are used to post the Transaction to the Account. The Transaction cannot be disputed on the grounds of the Exchange Rate applied.

12. INSURANCE

(The Bank plans to introduce this service in 2027 and will notify Clients separately)

12.1. Purchases made with the Card are insured in accordance with the Purchase Insurance Terms and Conditions. Tickets purchased with the Card are insured in accordance with the Ticket Insurance Terms and Conditions. These Terms and Conditions are available in the "Documents" section of the Bank's website and at the Client Service Centre.

12.2. Holders of Gold Credit Cards are covered by travel insurance in accordance with the Travel Insurance Terms and Conditions, which are available in the "Documents" section of the Bank's website and at the Client Service Centre.

12.3. If the Client has been issued two or more Cards, insurance cover is limited to the terms and conditions applicable to the Card with the highest sum insured. This means that having multiple Cards does not increase the total insurance cover.

13. INVESTIGATION OF TRANSACTIONS

13.1. After receiving information from the Client under Clause 4.9 of these Terms and Conditions, the Bank will check whether:

- the Cardholder has given their Consent to the Transaction;
- an incorrect Transaction has been made on the Account;
- the Commission Fees have been calculated correctly;
- any other error has occurred.

13.2. The Bank handles disputes in accordance with the rules of the International Card Organisations. The Client must cover any costs incurred by the Bank in carrying out the Client's instructions or reviewing Transactions made by the Client.

13.3. The Bank will not refund the amount debited as a result of a Transaction if its investigation confirms that the Transaction was properly authorised, was not incorrect or that the amount was debited from the Account for other valid reasons.

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

13.4. If Consent to a Transaction has been given in any of the ways described in Clause 4.7 of these Terms and Conditions, this is sufficient evidence that the Transaction was authorised. If the Transaction is disputed, this is also sufficient evidence that the Cardholder acted unlawfully or with malicious intent or failed through gross negligence to comply with the security requirements for using and keeping the Card and Authentication Methods set out in the Agreement.

13.5. If the Bank finds that a Transaction was unauthorised or incorrect when reviewing a dispute, it will refund the Transaction amount to the Client. The refund process follows the rules of the International Card Organisations. The Bank will refund the Transaction amount once it has recovered the funds from the International Card Organisation.

13.6. The Bank will review the Client's disputes concerning incorrect or Unauthorised Transactions made with Cards at the Bank's ATMs within 14 days of receiving the dispute.

13.7. The Bank may withhold funds or reserve amounts in the Client's accounts to secure its claims.

14. LIABILITY

14.1. The Client is fully responsible for complying with the Agreement and fulfilling their obligations under it. The Client is also responsible for ensuring that the Cardholder complies with the Agreement.

14.2. The Client must check their Account Statement in the Internet Bank at least once a month. The Client can also obtain an Account Statement from the Bank in accordance with the Pricelist. The Client must check that the information in the Account Statement is correct.

14.3. The Bank is not liable for Unauthorised or incorrect Transactions if the Client fails to report them to the Bank. The Client must inform the Bank as soon as they become aware of an Unauthorised or incorrect Transaction, but no later than 13 months after the funds were debited from the Account.

14.4. The Client is responsible for Transactions made until the Cardholder informs the Bank that the Card has been lost or stolen.

14.5. The Client is responsible for Transactions made with the Card during the 60 calendar days following its suspension.

14.6. The Client confirms that they have a lawful basis for providing the Cardholders' personal data to the Bank. The Client and the Cardholder acknowledge that the Bank processes personal data in accordance with the General Data Protection Regulation (GDPR) and the Privacy Policy.

14.7. Personal data is processed to issue and service the Card, carry out due diligence on the Client and the Cardholder, and comply with international and national sanctions requirements. Further information about the Privacy Policy is available here: https://bluorbank.lv/en/processing-of-personal-data.

14.8. If the Card is issued or used based on inaccurate, false or misleading information provided by the Cardholder, the Client is fully responsible for all obligations arising from the use of the Card.

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

14.9. The Client confirms that they understand their responsibility for providing inaccurate, false or misleading information. The Client also understands that leaving a required field blank means that the requested information does not exist.

14.10. Using the Card to make a Transaction or using Authentication Methods is evidence that the Cardholder has authorised the Transaction. It is also evidence that the Cardholder acted unlawfully or intentionally or failed through gross negligence to comply with one or more obligations under the Agreement concerning the use and safekeeping of the Card's security features.

14.11. The Bank will not reimburse losses of up to EUR 50 resulting from Unauthorised Transactions caused by the loss, theft or other unlawful misappropriation of remote banking tools (the Internet Bank, Authentication Methods or Mobile App) or the Card. This does not apply in the cases specified in the Payment Services and Electronic Money Law.

14.12. The Bank will not reimburse losses resulting from Unauthorised Transactions if the Client has acted unlawfully, with malicious intent or through gross negligence. This applies if the Cardholder has failed to use or keep remote banking tools (the Internet Bank or Authentication Methods) or the Card (including the PIN Code, password or username) in accordance with the Agreement or the instructions for using remote banking tools.

14.13. The Bank will also not reimburse losses if the Client fails to inform the Bank immediately upon becoming aware that an Authentication Method or the Card has been lost, stolen or otherwise unlawfully taken.

14.14. If the Client is a Consumer, the liability limit specified in Clause 14.11 of this Agreement does not apply.

14.15. If the Client makes Transactions without sufficient funds in the Account (an Unauthorised Credit Limit), the Client must pay Interest on the Unauthorised Credit Limit at the rate specified in the Pricelist.

14.16. The Bank is not liable for failing to carry out Cardholders' instructions, or for carrying them out incorrectly or incompletely, or for any errors, delays, inaccuracies or other problems resulting from incomplete or incorrectly completed documents or instructions submitted by Cardholders.

14.17. The Bank is not liable for failing to carry out Cardholders' instructions, or for carrying them out incompletely, if this is caused by a third party. The Bank is also not liable for losses caused by communications service providers.

14.18. The Bank is not liable if third parties refuse to accept the Card. The Bank is not responsible for the quality of goods or services purchased using the Card or for any restrictions imposed by third parties that may affect the Cardholder's interests.

14.19. By signing the Agreement, the Client confirms that they understand the risks associated with using the Card, including possible disruptions to communications or technical connections. Such disruptions may prevent Cardholders' instructions from being carried out or may result in their incomplete execution, provided that the disruptions were not caused by the Bank's gross negligence.

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

14.20. Neither Party is liable for partially or completely failing to fulfil its obligations under the Agreement if this is caused by force majeure events. These may include: amendments or additions to binding Laws and Regulations, or the adoption or entry into force of new Laws and Regulations, including sanctions, natural disasters and other natural events, military conflicts, strikes, disruptions to communications systems or information systems, and other circumstances beyond the Bank's control.

14.21. The Bank is responsible for the actions of its employees only to the extent that they act in the course of their duties and in accordance with instructions from the Bank's management.

14.22. The Parties agree that force majeure also includes the failure or partial failure of correspondent banks registered outside the member countries of the Organisation for Economic Co-operation and Development (OECD) to fulfil their obligations to the Bank, if this prevents or delays the Bank from fulfilling its obligations to the Client.

15. CHANGES TO THE AGREEMENT

15.1. The Bank may change the Agreement unilaterally. The Bank may also change Interest rates, the Pricelist and Transaction Limits. The Bank will inform the Client of these changes in writing using a durable medium. The Bank will give the Client 30 days' notice before the changes take effect, or 60 days' notice if the Client is a Consumer. The Bank may apply a shorter notice period if required by the authorities supervising the Bank.

15.2. The Parties agree that the Client is considered to have accepted the changes if they do not notify the Bank of their objections and request termination of the Agreement within 30 or 60 days, as applicable, after receiving the notice. The Bank may apply a shorter notice period if the changes to the Pricelist are favourable to the Client.

15.3. Each new version of the Agreement accepted by the Client after signing the original Agreement replaces the previous version, unless otherwise agreed.

15.4. The Client is responsible to the Bank for informing the Cardholder of any changes to the Agreement and the Pricelist.

16. TERM AND TERMINATION OF THE AGREEMENT

16.1. The Agreement takes effect when the Client has signed it and the Bank has approved it. It remains in force for an indefinite period. If the Agreement is concluded remotely and the Consumer signs it with an Electronic Signature, the Consumer has the right to withdraw from the Agreement within 14 days. The procedure for exercising this right of withdrawal is set out in the GTB.

16.2. The Bank may terminate the Agreement at any time by giving the Client at least 60 days' notice.

16.3. The Card's expiry date is not the expiry date of the Agreement. The Agreement only expires on that date if this is expressly stated in the Agreement.

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

16.4. When the Card expires, the Bank may decide not to renew the Card or continue the Agreement if:

- the Client owes fees for Card maintenance or has not used the Card for three consecutive months;
- the Client submits a written request to terminate the Agreement at least one month before the Card expires. The request can be submitted at the Bank or through the Internet Bank;
- the Client has an Unauthorised Credit Limit, meaning that they have spent more money than is available in the Account;
- the Bank finds that the Client or Cardholder has breached these Terms and Conditions;
- the Client has suspended the Card;
- the Account has been seized, payment transactions on the Account have been suspended, or funds are being deducted from the Account, in cases specified by Laws and Regulations;
- the Bank does not have accurate and complete information about the Cardholder.

16.5. If the Bank or the Client terminates the Agreement, the Client must repay any amounts owed to the Bank, including contractual penalties, any Unauthorised Credit Limit and Interest, if charged. The Client must also pay any other amounts due for using the Card and Account. All payments must be made in accordance with the Agreement and the Pricelist.

16.6. The Client has the right to request termination of the Agreement at any time. To do so, the Client must fulfil all their obligations in full and submit a written request to the Bank, either in person or through the Internet Bank, specifying all Cards they wish to close. If the Agreement is terminated, the provisions of the GTB concerning financial collateral apply.

16.7. The Agreement may only be terminated once the Client has fulfilled all their obligations. Termination must take place no later than 30 days after the request to terminate the Agreement has been submitted to the Bank.

16.8. The Agreement may be terminated at any time by mutual agreement between the Bank and the Client, subject to the requirements of Clause 16.7 of the Agreement.

16.9. The Bank may suspend the Card and terminate the Agreement at any time without prior notice to the Client or Cardholder if:

- the Client or Cardholder fails to fulfil their obligations to the Bank;
- the business relationship with the Client is terminated;
- the Client has suspended the Card. The Client has not reactivated or replaced it within 30 days. This period starts from the date the Card was suspended;
- the Client or Cardholder breaches Laws and Regulations when making Transactions;
- the Client's business activities have been suspended or terminated, or there are signs of insolvency, or an application to initiate insolvency proceedings has been filed with a court;

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

- the Bank has information indicating that the Client has a poor reputation, or the Client behaves disrespectfully towards the Bank;
- the Client or Cardholder has attempted to commit or has committed fraud against the Bank or any of its clients;
- the Bank suspects that the Cardholder has not agreed to have a Card issued in their name or no longer wishes to use the Card;
- the Client has submitted forged documents or provided false information to the Bank. In this case, the Bank may request that criminal proceedings be initiated against the person who provided the false information;
- the Bank has information or suspects that the Client has engaged in or attempted to engage in activities involving money laundering or terrorism and proliferation financing, or has committed another criminal offence. Money laundering means attempting to conceal the origin of money obtained through criminal activities. Terrorism and proliferation financing means providing funds to support terrorism or the proliferation of weapons.
- third parties have made claims against funds held in the Account or any other account opened in the Client's name with the Bank.
- at least one of the following conditions applies:
  - the Client fails to provide the Bank with accurate information and documents required to carry out due diligence on the Client in accordance with the Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing, or in other cases specified in that Law and the GTB.
  - the Bank decides to terminate the business relationship or demand early performance of obligations in the cases and in accordance with the procedures specified in the Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing. This also applies to other Bank clients who have the same beneficial owners and belong to a group connected with the Client. Beneficial owners are individuals who benefit from a company or Transaction.

In this case, the Client must pay any contractual penalties, any Unauthorised Credit Limit and any other amounts due for using the Card and Account. All payments must be made in accordance with the Agreement and the Pricelist, within the period specified in the Bank's notice.

16.10. The Bank may also terminate the Agreement in other cases specified in the GTB or Laws and Regulations.

16.11. If the Bank terminates the Agreement, the Client must pay the Bank all amounts due under the Agreement and the Pricelist after receiving the Bank's notice. These payments must be made within the period specified in the notice or the Agreement.

16.12. The Bank may terminate the Agreement unilaterally if it stops issuing Cards of this type.

17. DISPUTE RESOLUTION

17.1. If a dispute arises between the Client and the Bank, the Bank will try to find a mutually acceptable solution. To assess the matter giving rise to the dispute as thoroughly as possible, the Bank requires the Client to submit a written complaint.

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

17.2. The procedure for submitting complaints is set out in the GTB.

17.3. If the Client and the Bank cannot reach a mutually acceptable solution, a dispute with a Consumer may be resolved by the courts of the Republic of Latvia in accordance with the laws in force in the Republic of Latvia. A dispute with a Client that is a legal entity will be resolved in accordance with the procedure set out in the GTB.

18. FINAL PROVISIONS

18.1. The Bank may refuse to issue a Card without giving a reason for its decision.

18.2. Section headings are included in the Agreement to make it easier to read. They must not be used to interpret the Agreement.

18.3. If the Client is a Consumer, they have the right to receive a copy of the Agreement or information about specific terms of the Agreement, free of charge and upon request, on paper or another durable medium.

18.4. The Bank and the Client agree that, where applicable Laws and Regulations allow the Parties to agree that certain legal provisions will not apply (for example, where the service user is not a Consumer), entering into this Agreement is considered such an agreement.

18.5. The Bank may apply changes to Exchange Rates immediately without prior notice. Information about these changes and the current Exchange Rates is available at the Bank's premises and on its website at http://www.bluorbank.lv.

18.6. The Client and the Cardholder acknowledge that the Bank checks whether the information provided is true, accurate and complete. The Bank may request additional information and confirmation from third parties without prior approval from the Client or Cardholder. The Bank may also process and disclose data to third parties where necessary to provide services and fulfil the Agreement and other Bank terms and conditions.

18.7. The Bank processes personal data in accordance with the Bank's Privacy Policy.

18.8. The Bank may transfer any of its claims arising from the Agreement to third parties. It may also transfer the Client's personal data for the purpose of debt recovery and collection.

18.9. The Bank and the Client, where the Client is not a Consumer, agree that Sections 58, 60, 61, 63, 64, 65, 66, 67, 69–70[1], Section 77(1), and Sections 85, 87, 88, 89 and 99 of the Payment Services and Electronic Money Law do not apply to their business relationship. The time limit for claiming compensation for losses set out in Section 84 of that Law also does not apply.

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