General Terms and Conditions for the Provision of Payment Services to Corporate Clients, Private Individuals, Sole Proprietors and Associations

OTP banka d. d. • Slovenska cesta 58 • 1000 Ljubljana • Entered in the Companies Register kept by the District Court of Ljubljana • Company reg. no.: 5860580000 • Share capital: EUR 150,000,000.00 • VAT ID no.: SI94314527 • www.otpbanka.si • info@otpbanka.si

Table of contents

1. Introductory provisions

The General Terms and Conditions for the Provision of Payment Services to Corporate Clients, Private Individuals, Sole Proprietors and Associations (hereinafter: the General Terms and Conditions) set out the rights and obligations of the Bank and the user in relation to:

- the provision of payment services through transaction accounts opened with the Bank;
- the use of the digital bank;
- payment instruments; and
- safe deposit boxes.

These General Terms and Conditions are issued by OTP banka d.d., Slovenska ulica 58, 1000 Ljubljana, Slovenia, SWIFT KBMASI2X, registered with the District Court of Maribor, entry no. 062/10924200, company reg. no. 5860580000, VAT ID no.: SI 94314527 (hereinafter: the Bank). The Bank is included in the list of banks and savings banks authorised by the Bank of Slovenia to carry out payment services; the list is published on the Bank of Slovenia's website. The Bank of Slovenia is authorised to supervise the Bank.

2. Definitions

The terms used in these General Terms and Conditions have the following meaning:

Authentication means a procedure which allows the payment service provider to verify the identity of a payment service user or the validity of the use of a specific payment instrument, including the use of the user's personalised security credentials.
Authorisation is a process by which the provider of goods and services or an ATM obtains confirmation from the Bank allowing it to execute the transaction.
Automatic overdraft in the transaction account means the authorised disposal with funds in excess of the positive balance on the transaction account, provided that the user meets the Bank's terms and conditions.
Bank@Net com is an online bank allowing the user to use online banking services with an online application accessible via the Bank's website.
ATM is an automated electronic device by means of which the payment card holder can withdraw cash from their transaction account and execute other cash transactions.
SEPA B2B DD scheme sets out the rules, standards and procedures for executing SEPA direct debits where the payer and the payee are legal persons, sole proprietors or private individuals.
Contactless transaction is a quick, secure and simple transaction; it is made by tapping the card against the designated area of the POS terminal. Transactions up to a certain amount do not require entering the PIN. This amount varies from one country to another; the amount valid for Slovenia is published on the Bank's website.
CRS stands for the Common Reporting Standard for financial accounts for the purpose of taxation.
Fee Schedule is the Fee Schedule for Corporate Clients, Private Individuals, Sole Proprietors and Associations applicable at the time, available online at otpbanka.si/cenik-splosni-pogoji.
CVV is a three-digit verification number printed on the back of the card next to the signature strip.
Cross-border payment transaction is a payment transaction where the payer's payment service provider and the payee's payment service provider provide payment services to the payer or the payee in the territory of different Member States. A payment transaction is also executed as a cross-border transaction if the same payment service provider provides payment services to a payer in one Member State and to a payee in another Member State.
Value date is the reference period used by the Bank for accounting interest on funds debited or credited to the payment account.
Debit card is a card with immediate debit to the transaction account or with reservation of funds on the transaction account (e.g. VISA business debit card).
Business day is any day on which the payer's payment service provider or the payee's payment service provider participating in the execution of a payment transaction is open for business and enables its user to execute payment transactions.
Digital bank is the umbrella term for Bank@Net, Poslovni Bank@Net, eBank@Net com electronic bank, Bank@Net com online bank and mBank@Net com mobile bank.
Direct debit (SEPA DD) is a payment service where the payee orders a payment transaction to debit the payer's payment account based on the payer's mandate.
Additional card is a card issued to the authorised person of a contracting party based on an application of the contracting party or based on an application of the contracting party's authorised person by prior consent of the contracting party.
Debtor is a person that has past due payment obligations to the Bank.
Domestic payment transaction is a payment transaction where the payer's payment service provider and the payee's payment service provider or the single payment service provider provide payment services to the payer and the payee in the territory of the Republic of Slovenia;

Other payment transactions are transactions made in any currency if the payment transaction is made by transfer of funds between at least one payment service provider providing payment services in the territory of the Republic of Slovenia and a payment service provider providing payment services in the territory of a third country or in the territory of the EU using the currency other than the Member State's currency.
Member State is a European Union member state or a state signatory of the European Economic Area Agreement.
eBank@Net.com is an electronic bank allowing the user to use e-business services that are used with a stand-alone application for PCs.
E-unsubscription is an electronic form to unsubscribe from receiving e-documents, which the Bank of the e-document recipient forwards to the issuer of the e-document.
E-return receipt is an e-document with which the final recipient of the underlying e-document can reject or confirm the acceptance of each type of underlying e-document.
E-subscription is an electronic form to subscribe to receiving e-documents, which the Bank of the e-document recipient forwards to the issuer of the e-document.
Unique identifier means a combination of letters, numbers or characters assigned by the payment service provider to the user and used in the payment transaction for an unambiguous identification of the user and their payment account.
FATCA (Foreign Account Tax Compliant Act) means the law on compliance with tax regulations related to foreign accounts
Fiduciary account is a transaction account opened by the holder on their behalf but for the account of one or more third parties. The Bank can open a fiduciary account if the conditions stipulated by the Payment Services, Electronic Money Issuing Services and Payment Systems Act (hereinafter ZPlaSSIED) are met.
FLIK is a domestic interbank scheme that enables payments with instant settlement, approval of the payee's account and forwarding confirmation to the payer from the payment account.
(Transaction) account holder is a legal person, private individual, sole proprietor or association for whom the Bank opens a transaction account in accordance with the General Terms and Conditions for purposes of executing payment transactions and for other purposes associated with the use of banking services.
Card holder is a natural person authorised by a contracting party to be provided with and to use a payment card in accordance with these General Terms and Conditions.
Prepaid account holder is a legal person, sole proprietor, private individual or association for whom the Bank opens a prepaid account based on the application for a prepaid card.
Internal payment order is a payment order that is credited to transaction and other bank accounts.
Safe deposit access card is an identification document intended for the identification of the renter of the safe and any of their authorised persons, upon accessing the safe.
Special transaction account overdraft means the disposal with funds in excess of the positive balance on the transaction account, based on the concluded credit agreement.
Charge card is a payment card where the contracting party repays the total card debt once per month on the chosen day.
Card account is the account to which all card-based payments (primary and any additional cards) are debited.
Safe deposit box key is a key that the renter of the safe or any of their authorised representatives receives to open the safe.
Bank client is a legal person, sole proprietor, private individual or association that has a transaction account or technical accounts with the Bank for carrying out cash transactions.
Credit transfer is a payment service by which the payer makes an order to its payment service provider to make a single payment transaction or several payment transactions, including a standing order, from the payer's transaction account to the credit of the payee's transaction account.
Available account balance is the aggregate of credit balance in the transaction account (in domestic and foreign currencies) and authorised overdraft facilities available in the transaction account.
Qualified digital certificate is a computer record that contains information about the holder, the issuer of the digital certificate and the period of validity of the digital certificate.
Safe deposit access magnetic card is a card given by the Bank to the renter of the safe and any of their authorised persons to access the safe.
mBank@Net com is a mobile bank that a user installs on the smartphone.
SEPA bulk payment is a collection (bundle) of SEPA payment orders, executed by debiting the payer's account in the total amount of the bundle and authorising multiple accounts of one or more payees at their banks.
Mobile device is a mobile phone running the operating system Android or iOS, a tablet, a wearable device (e.g. smartwatch) or other device that allows for the installation and use of the mobile bank application and enables data transfer between the mobile device and POS terminal without direct contact (NFC technology) or by reading the QR code with a camera.
Mobile wallet is the Bank's application or an application of another provider that a user can install on their mobile device and add to it their payment cards in digital form for the purpose of paying for goods and services.
Mobile token is a system for generating passwords via the mBank@Net com application.

Strong customer authentication is authentication with the use of two or more elements that belong in the category of the user's knowledge (something only the user knows), the user's ownership (something only the user possesses) and inseparable connection with the user (something that the user is) that are independent of each other, which means that the violation of one element does not diminish the reliability of the other elements and that they are conceived so as to protect the confidentiality of data being verified.
Mailbox is a tab within the Poslovni Bank@Net application that allows importing and sending files with e-documents, SEPA bulk payments and SEPA direct debits, opening and changing letters of credit, topping up and emptying VISA prepaid business card, receiving e-invoices, notifications of marketing campaigns and news, and other messages by different types of transactions (Moneta, deposits, loans, cards, securities, etc.).
Renter is the contracting party who has concluded a Safe Deposit Box Rental Agreement with the Bank.
Rental fee is the amount set out in the Fee Schedule payable by the renter for the rental of the safe deposit box, and depends on the size of the safe deposit box and the rental period.
Account activity notification is the service involving sending SMS and/or e-mail messages with information on the balance of, inflows to/outflows from the transaction account, the expiry of deposit, the expiry of transaction account overdraft, successfully processed and/or declined payments or SEPA direct debits received.
Personalised security credentials are personalised features provided by the payment service provider to a payment service user for the purposes of authentication.
Personal password is a combination of a sequence of characters (identification number) chosen by the user themselves.
Bundle is a product set combining payment services and digital banking services.
PBN is an abbreviation for Poslovni Bank@Net.
PIN (Personal Identification Number) is the personal identification number that consist of four characters.
Business payment card is a payment card issued by the Bank at the request of the contracting party for use by authorised card holders that can be used to make payment transactions at ATMs, (online) POS, and to pay with the mobile wallet.
Poslovni Bank@Net is a method of conducting banking services online.
Payment account is the account opened by the payment service provider on behalf of the user that is used for executing payment transactions.
Payment services are the activities allowing:
- Deposit of cash to the transaction account and all activities required to manage this account;
- Withdrawal of cash from the transaction account and all activities required to manage this account;
- Execution of payment transactions to the credit and debit of the transaction account;
- Execution of payment transactions using funds extended as a loan to the user;
- Issuance of payment instruments and/or acquisition of payment transactions;
- Execution of money orders;
- Payment initiation services;
- Account information services.

The payment services referred to in indents 3 and 4 of the preceding paragraph include the execution of payment transactions by direct debit, by payment cards or similar devices or by credit payments.
Payment transaction is a deposit, transfer or withdrawal of funds based on the order of the payer or the order issued on behalf of the payer or the order of the payee, where the execution of such payment transaction through the payment service provider is independent of the basic obligations between the payer and payee.
Remote payment transaction is a payment transaction ordered through the Internet or a device that can be used for distance communications.
Payment instrument means any device or set of procedures or both, agreed upon between the user and their payment service provider, and it pertains to this user only for the purpose of initiating a payment order.
Payment order is an instruction by which the payer or the payee instructs their payment service provider to execute a payment transaction.
Payer is any legal person, private individual, sole proprietor or association that orders a payment transaction by issuing a payment order or approving the execution of a payment order issued by the payee.
Sole proprietor is a natural person independently performing their gainful activity in the scope of an organised company.
Contracting party is a legal person, private individual, sole proprietor or association who has concluded an agreement on opening and managing a transaction account, safe deposit box rental agreement, Visa business card agreement or other agreement with the Bank.
Agreement is a collective term used in the General Terms and Conditions to refer to an agreement on opening and managing a transaction account, safe deposit box rental agreement, Visa business card agreement or any other agreement concluded between a legal person, private individual, sole proprietor or association and the Bank.
Payment service provider managing an account is the payment service provider providing and managing a payment account for the payer.
Payment initiation service provider is a payment service provider performing payment initiation services.

Authorised person is a person authorised by the contracting party to represent it and conduct specific services.
POS terminal is an electronic device designed for the electronic transmission of data between a point of sale, a processing centre and the Bank in a card transaction.
Special zero balance accounts are accounts that national budget users hold with banks and savings banks designated by the Ministry of Finance. A zero balance account is used exclusively for cash withdrawals and deposits and has zero end-of-day balance.
Prepaid card is a debit card that a card holder can use to make payments within the available prepaid account balance.
Prepaid account is an account linked to the prepaid card and to which the contracting party's card payments are credited or debited.
Payee is any natural or legal person that is the intended recipient of funds subject to the payment transaction.
Application form is a declaration of intent to conduct services through Poslovni Bank@Net.
Default payment instrument is the payment instrument (payment card) that the card holder or mDenarnic@ user selects as the primary payment instrument for payment transactions (applies only to mobile devices running the Android operating system).
Processing centre is a business entity that is party to an agreement with the Bank for the processing and transfer of data in a payment card-based transaction.
Point of sale is the provider of goods and services that accepts payment cards as the payment method. A point of sale is equipped with a label of the payment card brands it accepts.
Registration is the process that the user carries out in the mobile wallet before the first use of the Flik service or before the first use of the mobile wallet.
Safe deposit box is a special metal drawer built into a secure and protected area of the Bank for storing belongings.
SEPA means Single Euro Payments Area.
SEPA direct debit or SEPA DD or SDD is a payment service where the payee makes an order to debit the user's payment account based on the user's mandate.
Consent to execute payment transaction is the delivery of a paper or electronic payment order by the user to the Bank or the payment initiation service provider, or delivery of authorisation for the execution of a payment transaction by the user in case the payment transaction is ordered by the payee or the payment initiation service provider.
Bank's website/URL is otpbanka.si.
Payment initiation service is the service of initiating a payment upon the order of the payment service user in relation to a payment account open with another payment service provider.
Account information service is an Internet service providing consolidated information about one or more payment accounts held by the payment service user with one or more payment service providers.
Standing order is an instruction by which the payer instructs their payment service provider to execute credit transfers regularly or at previously determined dates.
Durable medium is any instrument allowing the user to store information addressed to them personally in such a way as to make the information accessible for as long as necessary to allow future use of information and allowing unchanged reproduction of the information stored.
Transaction account or TA is a payment account opened by a bank or a Member State bank subsidiary registered in the Republic of Slovenia on behalf of one or more users to execute payments and for other purposes relating to the provision of banking services to the user.
Third country is any state other than an EU Member State or a signatory state to the European Economic Area (EEA) Agreement.
Third-party payment service provider is a non-bank payment service provider that provides payment initiation service and/or information on accounts opened with a bank.
Universal payment order (UPN) is a payment form used for the following payment transactions in EUR within SEPA: non-cash payments, cash payments, cash deposits and cash withdrawals.
User is any natural or legal person, private individual, sole proprietor or association using payment services as a payer or a payee or both who is party to an agreement on opening and managing a transaction account or other agreement concluded with the Bank.
User name is a randomly selected sequence of characters set by the Bank that does not change.
Database controllers are the Bank and the processing centre, which collect, process, and store data on card holders for the purposes of issuing and facilitating the use of payment cards.
Bank transfer schedule means the Schedule of domestic, cross-border and other payment transactions applicable at the time, which is published on the Bank's website.
Secure password is the password used by the card holder in a secure environment to confirm their identity in an online store equipped with the Visa Secure logo.
SMS Alert is the SMS transaction alert service for transactions on payment cards.
Depositor is the holder of a deposit or, in the case of a joint account, each of the holders of the deposit in accordance with the Deposit Guarantee Scheme Act (ZSJV).

Temporary deposit account is an account for legal persons in the process of being incorporated and registered in the Court Register to pay cash contributions.
Mobile device locking means the locking by way of a security element: PIN, fingerprint or pattern.
Private individual is any natural person other than a sole proprietor who independently conducts a registered activity or activity provided by law, such as notary, medical doctor, lawyer, farmer, and similar.
Confidential information is any information, facts and circumstances about a particular user, including personal data held by the payment service provider or participant in the payment system.
ZSJV is the abbreviation used in these General Terms and Conditions and stands for the Deposit Guarantee Scheme Act.

3. Transaction account

3.1 Transaction account opening

The Bank shall open a transaction account (TA) on the basis of a concluded Agreement on opening and managing a transaction account. To open a transaction account, in addition to the documentation listed below, the user's Slovenian tax number must also be provided.

When submitting the application to open a transaction account, the user shall:

- Submit documents that enable identification of the user and persons authorised to dispose with the funds in the account and conduct transactions, in compliance with the regulations, including the law governing the prevention of money laundering and terrorist financing and the provisions of the international agreement between the Republic of Slovenia and the USA regarding the Foreign Account Tax Compliance Act (FATCA);
- Deliver documents aimed at establishing a residence status for tax purposes in accordance with the OECD Standard for Automatic Exchange of Financial Account Information (Common Reporting Standard – CRS) and the Tax Procedure Act (ZDavP);
- Submit all data required for keeping a register of accounts, other documentation in accordance with applicable regulations, and any other documents required by the Bank.

The Bank shall either approve or reject the application no later than five (5) business days after receiving the application to open the transaction account with the documents requested. The Bank shall not be obligated to state the reasons for rejecting the application. The user may start using the transaction account on the first business day after the day the account was opened. During the term of the contractual relationship with the user, the Bank reserves the right to assign a new transaction account number to the user and to notify them thereof in writing as set out in these General Terms and Conditions.

3.2 Types of transaction accounts

3.2.1 Business transaction account

Business transaction account is designed for legal persons, sole proprietors, private individuals, associations and clients who have concluded agreements on the provision of custody services.

3.2.2 Fiduciary account

Fiduciary account is a special business transaction account opened by the user on their behalf but for the account of one or more third parties. The Bank may open a fiduciary account if the legal conditions are met.

3.2.3 Zero balance transaction account

A zero balance transaction account is available to budget users and is used exclusively for cash withdrawals and deposits and must show an end-of-day balance of zero.

3.2.4 Temporary deposit account

A temporary deposit account is used to pay cash contributions as initial capital of the company and other legal person in the amount specified in the respective articles of association, articles of incorporation or charter document. Based on the transfer of cash contributions, the Bank shall issue to the user, i.e. the company or other legal person being incorporated, a certificate of the payment of the contributions. The founder, as a natural person, shall transfer the contribution to the account of the company being incorporated in their own name, in cash or non-cash, while the founder, as a legal person, shall transfer the contribution to the account of the company being incorporated in its own name and only as non-cash contribution.

3.3 Transaction account managing

The Bank manages a transactions account in the domestic currency and in the currencies included in the reference exchange rate table of the ECB or the Bank of Slovenia. Currency exchange is carried out in accordance with Bank regulations and provisions. The Bank shall have discretion in deciding on whether to manage transaction accounts in foreign currency.

The Bank undertakes to carry out payment services for the user through their transaction account within the available transaction account balance. The credit balance on the transaction account is treated as a demand deposit with the Bank that manages the transaction account.

Only the user shall be entitled to dispose with the funds in the transaction account. The funds may be disposed with without restriction within the available transaction account balance, except where otherwise provided by law.

As a rule, cash withdrawals in excess of EUR 2,000.00 must be notified by the user to the branch at least one day in advance or by 11 a.m. on the respective day. Cash withdrawal in excess of EUR 2,000 via the digital bank must be notified by the user at least 2 days in advance. Upon notifying the cash withdrawal or on the day of the cash withdrawal, no order by a court or other authority may apply that prevents the user from disposing with the funds in the transaction account.

The user shall not assign, pledge or otherwise dispose with their rights and/or receivables arising from the Agreement on opening and managing a transaction account.

3.3.1 Transaction account authorised parties

The user may authorise in writing one or more parties to dispose with the funds in their transaction account. The authorisation shall be signed by the user before a bank employee or the signature on the authorisation shall be certified. The authorised party must, in addition to other necessary documentation as per the law on preventing money laundering and other internal rules of the Bank, also provide a Slovenian tax number.

The authorised party may not delegate the authorisation to another person, revoke the authorisation of other authorised persons, or terminate the agreement on opening and managing a transaction account, or close the transaction account.

The parties authorised to dispose with the funds in the transaction account must deposit their signatures with the Bank.

The authorisation remains effective until revoked in writing or until the Bank receives a formal notification on the winding up or an official notice of death of the authorised party, irrespective of any entry of changes of the right of disposal or representation made in any public register, as well as in case bankruptcy proceedings are initiated against the user, if a liquidator is appointed in case of regular dissolution of the user, in case of winding-up or death of the user, and in all other cases set out in applicable law.

At the Bank's discretion, a change of the user's legal representative may be taken into account by the Bank upon receipt of a decision on appointment of a new legal representative, even if the registered change of the right of representation is not yet visible in the relevant register.

The user hereby authorises the Bank to reverse any incorrect credits or debits to the transaction account caused by an error on the part of the Bank (double booking, etc.) and that were not ordered by the user, by way of a counter-booking so that the transaction account balance remains unchanged. The Bank shall notify the user thereof in the transaction account statement sent in the agreed manner. If the user objects to such a correction, the Bank will reinstate the transaction account balance to the balance preceding the correction and exercise its claim on the user in another way.

3.3.2 Disposal with the funds in the transaction account

In case of a payment transaction to the benefit of the user that is ordered by the payer, the Bank, acting as the user's payment service provider, shall make the funds in the user's transaction account available to the user as soon as the amount of the payment transaction intended for the user has been credited to the account of the Bank as the payee's payment service provider. In case of insufficient available balance to execute the payment transaction, and if the Bank makes the balance available to the payee after the approval of the amount of the payment transaction in the account of the Bank as the payee's payment service provider, the payee issues to the Bank a standing and irrevocable order or irrevocably authorises the Bank to withhold the funds received or

to debit the payee's transaction account for the amount of the payment transaction until the balance required is provided.

The Bank provides the following services in the transaction account:
- using the Visa business debit card;
- deposit and withdrawal of cash to transaction account;
- making payment transactions to and from the transaction account;
- standing order transactions;
- use of the digital bank, payment card transaction alert and notification of account activity;
- Sepa direct debits.

A building manager may keep reserve funds on behalf of commonhold owners of a multi-apartment building on a fiduciary account opened for each respective building and may only keep funds for several buildings on the same account upon the Bank's explicit consent. If commonhold owners adopt the decision to allow payments from the reserve fund only upon prior approval by one of the commonhold owners (authorised commonhold owner), the Bank will keep such balances in a separate fiduciary account kept for each building separately. The building manager is required to present to the Bank a decision of commonhold owners designating one or more persons as the authorised commonhold owner(s). Each payment order shall be approved by the building manager and one of the authorised commonhold owners. Notwithstanding any other provisions set out in these Terms and Conditions, payment orders can be debited against such a fiduciary account only via eBank@Net electronic bank, Bank@Net online bank, and mBank@Net mobile bank (the use of other payment instruments and withdrawal of cash from a fiduciary account are not possible). The authorised commonhold owner is required to use eBank@Net electronic bank, however, they shall be authorised only to confirm payment orders and export payment orders prior to confirmation and shall have no access to fiduciary account activity.

3.4 Execution of payment orders and notification of users

3.4.1 Issue of UPN forms

The user (hereinafter also referred to as the UPN issuer) shall issue a universal payment order (hereinafter: UPN) in accordance with the Instructions on the format, content and use of the UPN form published on the website of the Bank Association of Slovenia www.zbs-giz.si.

3.4.2 Receipt of payment order

The Bank shall execute a payment transaction when it receives the payment order, unless conditions exist for rejection of the payment order. It shall be deemed that the Bank received the payment order when a signed payment order is delivered to the Bank in a paper-based or electronic form, or through agreed communication channels, such as:

- payment order submitted at bank counter;
- payment order sent through digital bank;
- payment order transmitted through instant payment channels;
- payment order transmitted through third-party payment service provider.

Payment orders shall be completed in accordance with regulations, established payment system standards and these General Terms and Conditions. Payment orders shall contain the following essential elements:

- payer's name and address;
- payer's IBAN;
- amount and currency of payment;
- payee's name and address;
- payee's IBAN or account number;
- BIC for domestic payments or accurate name of the payee's bank in case of payments to third countries (these data are not required in case of domestic and cross-border payments);
- payment date;
- purpose of payment;
- purpose code for payment orders submitted on the UPN form;
- payer's signature;
- other information, if so requested by a special regulation.

Signature of the payment order shall be deemed to constitute consent to the execution of the payment order.

If the payment order is received by the Bank on a day other than a business day or if the payment order is received after the cut-off time, it shall be regarded as having been received on the first upcoming business day. If the date indicated on the payment order as the payment execution date refers to a later date, it shall be deemed that the payment order has been received by the Bank on the day of the payment order execution, provided that all other requirements for the execution of the order are met.

If the Bank receives a payment request from the payer in the form of a standing order or a direct debit, it shall be deemed as having been received on the day of execution of the standing order or a direct debit.

3.4.3 Execution of payment order

The Bank shall execute the payment order if the following conditions are fulfilled:

- The payment order is received by the Bank in line with the Bank transfer schedule;
- The transaction account balance is sufficient to execute the payment order;
- The payment order is signed, completed in a legible manner (without corrections) and contains all requested information required under the second paragraph of Chapter 3.3.2. of these General Terms and Conditions (Receipt of payment order);
- The user is not subject to sanctions or does not meet the conditions laid down in Chapter 5.2. (Sanctions) of these General Terms and Conditions;
- There are no legal and/or internal impediments or restrictions for the execution of the payment order.

The payment order may not contain a condition precedent or subsequent. Should the payment order contain a condition precedent or subsequent, it shall have no legal effect.

In the absence of any special instructions given by the user, the Bank shall use its best judgement to determine the manner for executing the payment order to the credit of the user. Receiving such a payment does not yet trigger any rights or claims of third parties on the Bank.

The user shall be responsible for the accuracy and completeness of data on the payment order. The Bank shall not be liable for any damage incurred by the user as a result of the execution of falsified, modified or incorrectly completed payment orders.

The user shall, immediately and without delay, notify the Bank of any unauthorised and/or incorrectly initiated or executed payment transaction when determining that such a transaction has been made. In any case, the user shall notify the Bank no later than in thirteen (13) months after the date of credit or debit.

If the date determined on the payment order as the payment execution date refers to a later date, the Bank shall verify the conditions for the execution of the order on that day. Deadlines for the execution of payment transactions are defined in the Bank transfer schedule.

Payment orders with a past due value date shall be executed within the funds available according to the stated priorities, and considering the same priorities, according to the FIFO method (first in, first out). In doing so, the Bank shall observe the priorities stipulated by law.

The first payment order that cannot be executed due to insufficient transaction account balance shall suspend the execution of the remaining payment orders until funds are provided in the user's transaction account.

The Bank shall not verify the purpose code and shall forward it to the payee in the form as stated by the user. Neither shall the Bank check whether the account number matches the payee specified by the user. The Bank assumes no responsibility for inappropriate processing of a payment transaction, if the user or the authorised person does not use the payment purpose code corresponding to the actual purpose.

The Bank assumes no responsibility for the effects of the transactions between the user and the payee that give rise to the payment transaction. The user is responsible for the decisions taken in connection with the conclusion of the transaction and for the credit rating assessment and other circumstances on the part of the payee. If the user orders a payment transaction for the purchase of and trading in financial instruments or any other form of investment, the Bank shall not be liable for any financial effects arising from the transactions concluded. It is the user's responsibility to make independent enquiries on their own regarding the financial instruments or other services which are the subject of their investment decision.

In accordance with SEPA rules, a simultaneous transfer of the structured reference and the text denoting the payment purpose at the interbank level is not possible. If a credit reference is entered in the payment order, the

Bank provides the payee with information about the reference and the purpose code without the text denoting the payment purpose.

For a standing order or a direct debit to be executed on the agreed date, funds must be available on the transaction account at least one business day prior to the anticipated execution (except for standing orders for the transfer of daily account balances which are, in accordance with the Bank transfer schedule, executed at the end of the business day).

If a payer presents to the Bank for execution a paper-based payment order with QR code, the Bank may forward to the payee and their bank only the information included in the QR code. The Bank is not obligated to check whether the QR code matches other data in the payment order.

The Bank will execute a payment transaction based on an executable enforcement order or any other decision issued by the competent authority without consent of the user or authorised person, in accordance with the legislation applicable at the time.

The Bank shall charge the user a fee for the execution of the payment order in accordance with the Bank transfer schedule applicable at the time. The amount of the fee varies depending on the type of communication channel through which the user orders the payment transaction (e.g. at a bank counter, at an ATM, via a digital bank, at a post office counter).

The Bank shall inform the user about the change of the Bank transfer schedule by means of announcements on the Bank's website, in its branches and via e-bank.

3.4.4 Rejection of payment order

The Bank may reject the execution of the payment order if any of the conditions for the execution specified in these General Terms and Conditions is not met. The Bank shall inform the user of the rejection and, if possible, of the reasons therefor and the procedure for eliminating errors that led to the rejection, unless such is prohibited by other regulations. If the wrong transaction account of the payee is stated in the bulk payment package or the transaction account has already been closed, the Bank will reject the entire bulk payment package and the user will have to resubmit the package for execution.

In case of instant payments, the Bank may reject the execution of a payment order when detecting sanctions risks.

The Bank shall submit, or make available, the notification referred to in the first paragraph of this Article to the user as soon as possible, and at the latest by the deadline set for execution of the payment order referred to in Chapter 3.3.3. (Execution of payment order) herein.

The Bank may charge the user a fee for notification of payment order rejection in accordance with the Bank transfer schedule applicable at the time.

3.4.5 Revocation of payment order

The user may revoke the payment order at any time by:

- Revoking consent for the execution of the payment transaction or a batch of payment transactions;
- Requesting the payment order to be returned;
- Cancelling the electronic payment order sent;
- Revoking the authorisation for the standing order or direct debit.

Any payment transaction executed after the revocation shall be considered unauthorised. The user can revoke the payment order no later than by the end of the business day preceding the payment date.

Notwithstanding the first paragraph of this Chapter, the user cannot revoke the payment order after the payment order for the execution of the payment transaction became irrevocable, i.e. when it was received by the payee's bank. If the payment transaction is initiated by a payment initiation service provider, by the payee or by the user through the payee, the user cannot revoke the payment order after they have given consent to the payment initiation service provider to initiate the payment transaction or after they have consented to the execution of the payment transaction to the credit of the payee.

Notwithstanding the preceding paragraph, in cases where the payment transaction is ordered by the payee through a SEPA direct debit, the user may revoke the payment order initiated by the payee by the end of the business day before the agreed date of debit to the user's account.

After the expiry of the deadlines for payment order revocation referred to in this Chapter, the user may revoke the payment order only based on agreement with the Bank. If the payment transaction is ordered by the payee or by the user through the payee, the revocation of the payment order after expiration of the stated period needs to be authorised by the payee as well.

A payment order the execution of which the user has agreed with the Bank to start on a specific day or at the end of a specific period or on the day on which the user makes funds available, may be revoked by the user until the end of the business day on which the execution of the payment order was agreed to start.

The Bank may charge the user a fee for the revocation of the payment order in accordance with the Bank transfer schedule applicable at the time.

3.4.6. Request to revoke executed payment order

A revocation of an executed payment order may only be requested in the case of duplicated transaction, technical problems or abuse. The user shall send the Bank a written request to revoke a payment order that has already been executed no later than in thirteen (13) months of the date of order execution.

The user shall be reimbursed for the amount only with consent of the payee. The amount reimbursed may be reduced by the sum of charges made by the payee's bank and any other fees of intermediary banks.

If the Bank receives a written request for revocation from another bank, it shall notify the user (payee) of having received the payment revocation request (consent). The user shall confirm or reject the request for revocation in writing in eight (8) days. If the request is confirmed, the Bank shall reimburse the sum to the payer. If the request is rejected or the user does not respond to it, the Bank will not reimburse the payment.

3.5 SEPA direct debit (SEPA DD) for the user - payer under the basic scheme

3.5.1 Mandate

The payer and the payee agree on settling of the user's obligations by means of SEPA DD whereby the payer issues mandate to the payee for executing SEPA DD.
The payer shall notify the payee of any changes of information contained in the mandate and of revocation of the mandate. In executing SEPA DD, the Bank does not verify the existence and the content of the mandate.
The payer's mandate becomes void if the payee has not submitted any payment order to be executed via SEPA DD within 36 months after giving the mandate.

3.5.2 Executing SEPA DD payment orders

The Bank shall execute a SEPA DD payment transaction on the execution date, if the payer has provided sufficient funds in the transaction account according to the Schedule of domestic, cross-border and other payment transactions applicable at the time.
The payer may request their bank to discontinue or limit the execution of SEPA DD on their transaction account, in the form and content satisfactory to the Bank.

3.5.3 Objection

The payer may deliver to the Bank a written objection, requesting it not to execute the payment order, no later than one business day prior to the execution date. The written objection shall include at least the following information: mandate reference code, amount, execution date, and name of the payee.

3.5.4 Refund

The payer may request a SEPA DD refund, including fees and interest, for both authorised and unauthorised payments, in accordance with the applicable legislation and the SEPA Direct Debit Instructions published on the Bank's website.

The payer may submit a request for a SEPA DD refund only to the bank where SEPA DD was executed.

The payer may request a SEPA DD refund:

- No later than within eight (8) weeks of the executed SEPA DD, if the payer consented to the execution of the payment transaction without a specified amount, and if the amount of the SEPA DD exceeds the amount that could reasonably be expected by the payer given the amounts of past payment transactions, contractual terms and other circumstances in a given case, however, not if the excess amount is the result of a currency exchange;
- No later than within thirteen (13) months, if they have informed their bank that they have not consented to SEPA DD execution (unauthorised payment). In such case, the payer's bank requests from the payee's bank evidence of valid mandate. If the bank receives evidence of a valid mandate, it shall reject the refund request. If the Bank receives from the payer's bank a notification that a valid mandate does not exist or if it establishes, based on submitted evidence, that the mandate is not consistent with the SDD DD executed, it shall refund the funds to the payment account and submit a request for refund to the payee's bank. The payer may request refund of executed SDD DD no later than in thirteen (13) months also in the case of errors in SDD DD execution at the payer's bank.

Notwithstanding the preceding paragraph, the payer shall not have the right to claim refund of an executed SEPA DD if the payer gave mandate to the execution of a payment transaction directly to the payee and if the Bank or the payee in the agreed manner provided or made available to the payer information on the payment transaction at least fourteen (14) days before the due date.

3.5.5 Notification

The payer shall be informed of the amount and the date of each individual SEPA DD by prior notification from the payee. The Bank may allow the payer to consult the SEPA DD payment order or may provide the payer with information about SEPA DD payment order prior to the execution date.

The payer shall be notified of executed SEPA DD payment orders by means of the transaction account statement. The Bank shall promptly inform the payer of any non-executed SEPA DD payment orders by a special notice.

3.5.6 Complaints

The payer and the payee shall mutually resolve all complaints of the payer arising from their contractual relationship, whereas other complaints shall be resolved by the user with the Bank.

3.5.7 Fees

The payer shall pay the Bank a fee for SEPA DD execution and non-execution in the manner and in accordance with the applicable Fee Schedule. Payment of fees is regulated by Subchapter 3.19.2 of these General Terms and Conditions (Transaction account fees).

3.6 SEPA DD for the user under the B2B scheme

SEPA DD are executed in accordance with the SEPA Direct Debit Instructions published on the website SEPA Business - Direct Debit and Standing Order | OTPbanka and in accordance with these General Terms and Conditions.

3.6.1 Mandate

SEPA DD is a payment service where the payee orders a payment transaction to debit the user's transaction account based on the user's mandate. The user can change or withdraw the mandate only with the payee. The user shall inform the Bank of the mandate issued in the SEPA DD B2B scheme and deliver a copy thereof in due time, i.e. no later than one business day prior to the first debit to the transaction account. The user shall notify the Bank of any changes in the mandate or of its revocation.

The Bank shall cross-check the data in the mandate with the data in the SEPA DD payment order. The Bank will execute the SEPA DD, if the payer does not notify it of any change or revocation of the mandate.

The user's mandate becomes void if the payee has not submitted any payment order to be executed via SEPA DD within 36 months after giving the consent.

3.6.2 Executing SEPA DD payment orders

The Bank shall execute the SEPA DB payment transaction on the execution date if the user's transaction account has sufficient balance and there are no grounds for rejecting the execution. The execution date may be any banking day. If the execution date falls on a non-working day, the Bank shall execute payment orders on the first following working day.

The Bank shall refuse to execute a SEPA DB if the user has prohibited the execution of SEPA DB on their account; if the payee has indicated a user account on which the Bank does not execute SEPA DB; if the user's account is incorrect, blocked or closed; if the user has not provided mandate data or the mandate data do not match the transaction data; if the user has not provided sufficient funds in the account; if there are other reasons or an agreement between the Bank and the user.

The user may instruct their Bank to discontinue executing SEPA DD on their transaction account.

3.6.3 Objection

The user may deliver to the Bank a written objection, requesting it not to execute the SEPA DD payment order, no later than one business day prior to the execution date. The written objection shall include at least the following information: mandate reference code, amount, execution date, and name of the payee.

Payments under executed payment orders cannot be refunded.

3.6.4 Notification

The user shall be informed of the amount and the date of each individual SEPA DD by prior notification from the payee. The Bank may allow the payer to inspect the payment orders or provide the payer the information of payment orders prior to their execution date.

The user is informed about the executed payment orders in the statement of account. The Bank shall promptly inform the user of any non-executed SEPA DD payment orders by a special notice.

3.6.5 Fees

The user shall pay the Bank a fee for SEPA DD execution and non-execution in the manner and in accordance with the applicable Fee Schedule. Payment of fees is regulated by Subchapter 3.19.2 of these General Terms and Conditions (Transaction account fees).

3.7 Standing order

A standing order (hereinafter: SO) is a credit transfer:

- by which the user gives a written consent to the Bank to execute a single payment transaction in the domestic currency and foreign currencies, repeated in the same amounts and executed on a specific date;
- by which the user gives a written consent to the Bank to execute a single payment transaction in the domestic currency and foreign currencies in variable amounts, executed on a specific date;
- by which the user gives a written consent to the execution of a specific payment transaction in domestic and foreign currencies for the repayment of a liability to the Bank;
- by which the user gives a written consent to transfer the daily balance of the transaction account in the domestic currency to another account.

The Bank will accept consent for executing a standing order, if standing order is to be completed by at least two consecutive payments on a specific date in an agreed-upon chronological order or within the period of authorisation.

The Bank shall have the discretion to reject the request to open opening a standing order. The Bank shall execute accepted authorisations (opening, change, revocation) only if the user notifies it at least one business day prior to the execution of a standing order.

3.8 Business payment card operations

Each type of payment card listed hereinunder shall be subject to the provisions of this entire Chapter unless otherwise provided by respective subchapter of this Chapter.

3.8.1 Types of payment cards

The Bank issues the following business payment cards that include the contactless option:

- VISA business debit card;
- VISA business charge card;
- VISA business prepaid card.

3.8.2 VISA business debit card

The contracting party submits an application for the issue of a Visa business debit card (hereinafter: the card). The Bank may refuse the application for a card without stating the reason.

The card is a payment instrument used:

- **At a bank and post office**: when using the transaction account, the Visa business debit card is regarded as an identification card for the transaction account and as a bank payment card. For identification purposes, the user is also required to present a valid identity document with a photo at a bank or post office counter.
- **At points of sale with the Visa label in Slovenia and abroad**: the card holder initiates a payment order to credit funds to the account of the point of sale owner marked with the Visa label by:

  - inserting their card into the POS terminal or tapping it against the terminal and entering PIN; or
  - inserting their card into the POS terminal or tapping it against the terminal; or
  - inserting their card into the POS terminal or tapping it against the terminal and signing the transaction slip using the same signature as it appears on the card; or
  - swiping the magnetic strap through the POS terminal and signing the transaction slip using the same signature as it appears on the card.

  The card holder shall enable the point of sale seller to verify the validity of the card and the card holder's identity. The card holder may tap the card, hold the mobile phone close to the POS terminal (in case of mobile wallet), insert the card or enter the PIN only once per transaction. In the opposite case, the card holder must request a slip showing failed authorisation.

- **For cash withdrawal at ATMs with the Visa label in Slovenia and abroad:**
- **For remote purchases (e.g. phone sales, mail order), where the card is not physically at the point of sale, using the method accepted by the payee (several available options):**
  - by communicating the card number and the expiration date; or
  - by communicating the card number, the expiration date, and CVV number;

– **For purchases in online stores**, where the card is not physically at the point of sale, using the method accepted and selected by the payee (several available options):

  - by entering the card number and the expiration date; or
  - by entering the card number, the expiration date, and CVV number; or
  - by entering the card number, the expiration date and CVV number and confirming the payment in the mDenarnic@ mobile wallet or retail digital bank, if the card holder is the Bank's client (in accordance with the respective terms and conditions).

– **For ATM cash deposit:** the card holder must have a valid authorisation to deposit cash at an ATM. Otherwise, the Bank reserves the right to restrict the use of the card.

The following conditions have to be met for the approval of a card application:

- the contracting party does not have any overdue and outstanding liabilities to the Bank;
- the conditions relating to sanctions are not met;
- the contracting party has an open transaction account with the Bank.

The card can be issued to persons of legal age (card holder) who are authorised to use the business account by the contracting party. The card holder may either be the authorised person of the contracting party, legal representative of the contracting party, or an employee of the contracting party.

The card holder will receive the card and PIN known only to them. The card will be delivered to the card holder at the address of the contracting party's registered office and the PIN will be disclosed by SMS or sent by post to the address of the contracting party's registered office, if such is communicated to the Bank by the card holder upon ordering the card. The Bank shall send the card by ordinary mail. The PIN, if sent by post, shall be sent by registered mail. The Bank will send the card and the PIN in two separate parcels mailed on different days. If the parcel containing the card is returned to the Bank, the Bank will again notify the card holder that a card is available and ask them to collect it. The card must be collected in ninety (90) days of the order. After ninety (90) days the Bank will destroy the card. Immediately after receiving the card, the card holder shall sign it with a permanent pen. The card is not valid unless signed. The contracting party shall bear all the damage and costs arising from abuse of an unsigned card.

When using the transaction account, the card is regarded as an identification card for the transaction account and as a bank payment card. For card holder identification purposes, the user is also required to present a valid identification document with a photo.

The contracting party irrevocably agrees and authorises the Bank to debit its transaction account for the card issuing fee and other charges arising from card transactions.

When a card is ordered, the Bank will transmit the card holder's personal data (name, surname, mobile phone number, e-mail, etc.) to the external processing centre for the purposes of secure online transactions, payments at points of sale and ATMs, SMS transaction alert for payment card transactions, use of mobile wallet, and other services linked to payment cards.

The card is non-transferrable and may only be used by the card holder. If the authorisation to operate a business account is revoked, the contracting party shall hand over the card to the Bank, and the Bank shall destroy the card and prevent its use.

In cases where strong authentication is applied in remote purchases, such authentication includes elements for dynamic linking of the payment transaction with the specified amount and specified payee. The card holder confirms the online payment in the mDenarnic@ mobile wallet by entering their password or using their biometric data, or if the card holder is also the Bank's client, in the retail digital bank. The card holder shall verify the amount of the transaction and the name of the point of sale where they made the online purchase before confirming identity as part of the online payment. If data do not match, the card holder may not proceed with the confirmation and must notify the event to the Bank.

For remote and online purchases, the card holder must take special care to ensure that the security of the point of sale and payment is adequate before entering the card details. The card holder shall make purchases only on secure websites and only from reliable and verified sellers of goods and services. Before making a remote or online purchase, the card holder must always check the trustworthiness of the merchant and their references. The card holder is required to review the merchant's terms and conditions before executing the payment. The card holder shall enter the data specified as security mechanisms (expiration date, card number, security CVV number) only after they have made the online purchase, and they only need to execute the payment. The car holder must comply with all remote payment authentication requirements. The Bank shall not be liable for damage incurred by the contracting party as a result of a breach of the card holder's obligations set out in this paragraph.

The card holder shall ensure that the device they use to make payments without a card is protected against viruses and attacks. The Bank recommends that the card holder installs quality anti-malware software on the device, which is frequently updated automatically, activates a firewall on the device and regularly updates the operating system and other software installed on the device used to make online purchases. The card holder is responsible for selecting, using and maintaining the security system to protect the computer or mobile device used to make online purchases, and shall be fully liable for any damage incurred by them or the Bank as a result of malicious software on their computer or mobile device. The card holder must protect access to the device with a password or other appropriate protection and must never leave the device unattended. The Bank shall not be liable for damage incurred by the contracting party as a result of a breach of the card holder's obligations set out in this paragraph.

The card holder may carry out transactions within the approved limit and available balance in the contracting party's transaction account. The Bank will approve the amount of the monthly and daily limit for an individual card holder based on the maximum limit proposed by the contracting party. The Bank may unilaterally change the limit at any time, of which it shall notify the contracting party by means of a notice in the digital bank mailbox, by SMS, by post with or without statements or in any other manner agreed with the contracting party. If the contracting party does not agree with the amount of the limit, they may agree to change it in accordance with the Bank's business policy.

For security reasons the card holder shall make sure that all procedures at a point of sale are carried out in their presence. The card holder must have the card on them or under supervision at all times when making payments, they must not leave the card out of sight and must supervise the entire payment process at all times. The Bank shall not be liable for damage incurred by the contracting party as a result of a breach of the card holder's obligations set out in this paragraph.

The Bank shall not be liable for any failure by the point of sale to execute a payment transaction.

If the contracting party fails to ensure sufficient available balance prior to executing the transaction, the Bank is entitled to reject authorisation of the transaction.

The contracting party irrevocably authorises the Bank and gives the Bank a permanent and irrevocable order to use any of the contracting party's balance with the Bank to settle overdue and outstanding obligations arising from the use of the card, irrespective of the agreed maturity. The contracting party undertakes to provide, no later than by the due date, sufficient available balance to settle the liabilities incurred and fees associated with using the card. If the contracting party fails to ensure sufficient balance by the due date to settle the liabilities incurred, including fees and charges, they shall be charged the relevant default interest until sufficient balance has been made available. Default interest will be charged in the amount and using the method stipulated in the Bank's Resolution on interest rates applicable at the time.

If the liabilities are not settled in full, the Bank shall disable the use of the card entirely after ten (10) days. The expiry of the card shall have no impact on the contracting party's obligation to repay the liabilities arising from the use of the card incurred prior to the expiry of the card.

The Bank enables the card holder to use the SMS transaction alert service to enhance security of card use. The SMS alert message provides the card holder with information about the completed or rejected payment transaction on their mobile device. If the card holder receives an SMS alert about a payment transaction unknown to them and which was not made by the card holder, the card holder must block the card as soon as possible in accordance with Subchapter 3.8.8. (Lost, stolen or misused card) of these General Terms and Conditions. The contracting party must regularly monitor their payment card transactions through the digital bank or through the statements of transactions sent to them by the Bank. If they notice payment transactions that have not been made by the authorised person (unauthorised payment transaction), they shall inform the Bank as soon as possible. The Bank shall not be liable for damage incurred by the contracting party as a result of a breach of the card holder's obligations set out in this paragraph.

The card holder undertakes to treat the card, the card details and other security elements of the card with due diligence to prevent the loss, theft or misuse of the card. In the event of an unauthorised payment transaction resulting from fraud, intent or gross negligence on the part of the card holder, the contracting party shall be liable for all damage incurred.

The Bank shall not be liable for damage incurred by the contracting party as a result of a third party obtaining possession of the card or card data necessary to make an online purchase and using the card or card data for online store purchase, unless the card has been reported stolen or lost in accordance with these Terms and Conditions. The Bank shall not be liable for the quality of goods and/or services paid for by the card holder using the card. The Bank shall also not be liable for any defective performance of an agreement to purchase goods or services paid for with the card. The account holder or the contracting party is required to settle their obligations to the Bank irrespective of any dispute at the point of sale. The contracting party shall have the right to request a refund of payments made for online purchases directly from the point of sale to which the payment was made. Once a payment transaction is confirmed, it can no longer be cancelled or stopped. A purchase that has been confirmed by the card holder can only be cancelled at the point of sale where it was made.
If the card holder uses the card to pay for the purchase and for trading in financial instruments (shares, other securities), or uses the card for any online or other form of investment, or for the purchase of cryptocurrencies, the Bank shall not be liable for any financial effects arising from the transactions made. It is the card holder's or contracting party's responsibility to make enquiries on their own regarding the financial instruments or other services which are the subject of the investment decision.

3.8.3 VISA business prepaid card

The provisions of these General Terms and Conditions applicable to the Visa business debit card shall also apply to the use of the Visa business prepaid card (hereinafter: the card) to the extent that they are not in conflict with the provisions regulating the use of the Visa business prepaid card.

The contracting party shall submit a card application. The Bank may refuse the application for a card without stating the reason.

The following conditions have to be met for the approval of a card application:

- the contracting party does not have any overdue and outstanding liabilities to the Bank;
- the conditions relating to sanctions are not met;
- the contracting party has an open transaction account with the Bank.

The card can be issued to persons of legal age (hereinafter: card holder) who are authorised to use the prepaid account by the contracting party. The card holder may either be the authorised person of the contracting party, legal representative of the contracting party, or an employee of the contracting party.

Based on approved card application, the Bank will open a prepaid account for the contracting party to which the contracting party can deposit funds to be spent with this card, pay service fees, and compensate any exchange rate differences incurred by using the card.

The contracting party irrevocably agrees and authorises the Bank to debit its transaction account for the card issuing fee and other charges arising from card transactions.

The card holder will receive the card and PIN known only to them. The card will be delivered to the card holder at the address of the contracting party's registered office and the PIN will be disclosed by SMS or sent by post to the address of the contracting party's registered office, if such is communicated to the Bank by the card holder upon ordering the card. The Bank shall send the card by ordinary mail. The PIN, if sent by post, shall be sent by registered mail. The Bank will send the card and the PIN in two separate parcels mailed on different days. If the parcel containing the card is returned to the Bank, the Bank will again notify the card holder that a card is available and ask them to collect it. The card must be collected in ninety (90) days of the order. After ninety (90) days the Bank will destroy the card. Immediately after receiving the card, the card holder shall sign it with a permanent pen. The card is not valid unless signed. The contracting party shall bear all the damage and costs arising from abuse of an unsigned card.

When a card is ordered, the Bank will transmit the card holder's personal data (name, surname, mobile phone number, e-mail, etc.) to the external processing centre for the purposes of secure online transactions, payments at points of sale and ATMs, SMS transaction alert for payment card transactions, use of mobile wallet, and other services linked to payment cards.

The card is non-transferrable and may only be used by the card holder. If the authorisation to operate the business account is revoked, the contracting party shall hand over the card to the Bank, and the Bank shall destroy the card and prevent its use.

The card holder agrees to accident insurance for accidental death and permanent disability for the first year after card issuance with the insurance company Sava d.d. for the sum insured of EUR 2,086.46 in case of accidental death and EUR 4,172.92 in case of permanent disability. The General Terms and Conditions for accident insurance of payment card holders are available to card holders at any Bank branch office.

The contracting party shall provide funds in the prepaid account and thereby the funds needed to use the card and pay service fees and charges associated with the prepaid account and the card. The prepaid account is intended solely for using the Visa business prepaid card. The funds shall be provided by transfers using the account number and reference number given on the back of the card in accordance with these General Terms and Conditions.

The card holder may use the card within approved limits, i.e. the cash withdrawal amount is capped at EUR 350.00 per day and EUR 1,000.00 per month. The Bank may unilaterally change the limit at any time, of which it shall notify the contracting party by means of a notice in the digital bank mailbox, by SMS, by post with or without statements or in any other manner agreed with the contracting party. If the contracting party does not agree with the amount of the limit, they may agree to change it in accordance with the Bank's business policy.

The total amount of deposits to the prepaid account within a calendar month shall not exceed EUR 2,000.00 and the total prepaid account balance at any time is capped at EUR 2,000.00. If the cap is exceeded, the funds from the transaction account opened for the purpose of card operations shall not be transferred to the prepaid account, but will remain in the transaction account linked to the card.

The contracting party shall ensure sufficient balance on the prepaid account to settle all liabilities to the Bank arising from fees, costs, exchange rate differences and any transactions for which the merchant does not require authorisation that are incurred by using the Visa business prepaid card. If the funds in the prepaid account do not suffice for the repayment of liabilities, the contracting party hereby irrevocably authorises the Bank and gives it a permanent and irrevocable order to use any of the contracting party's balance in their transaction account in EUR to settle liabilities arising from the use of the card in Slovenia or abroad, irrespective of the agreed maturity. If the contracting party fails to ensure sufficient balance by the due date to settle the liabilities incurred, including fees and charges, they shall be charged the relevant default interest until sufficient balance has been made available. Default interest will be charged in the amount and using the method stipulated in the Bank's Resolution on interest rates applicable at the time.

If the liabilities are not settled in full, the Bank shall disable the use of the card entirely after ten (10) days. The expiry of the card shall have no impact on the contracting party's obligation to repay the liabilities arising from the use of the card incurred prior to the expiry of the card.

The funds in the prepaid account belong to the contracting party.

3.8.4 Visa business charge card

The provisions of these General Terms and Conditions applicable to the Visa business debit card shall also apply to the use of the Visa business charge card (hereinafter: the card) to the extent that they are not in conflict with the provisions regulating the use of the Visa business charge card.

The contracting party shall submit a card application. The Bank may refuse the application for a card without stating the reason.

The following conditions have to be met for the approval of a card application:

- the contracting party does not have any overdue and outstanding liabilities to the Bank;
- the conditions relating to sanctions are not met.

The contracting party shall conclude a Visa Business Card Agreement with the Bank. The contracting party shall pay an annual fee for each card issued. The amount of the annual fee and payment method are set out in the applicable Fee Schedule of the Bank.

The card can be issued to persons of legal age (hereinafter: card holder) who are authorised to use the business account by the contracting party. The card holder may either be the authorised person of the contracting party, legal representative of the contracting party, or an employee of the contracting party.

The contracting party irrevocably agrees and authorises the Bank to debit its transaction account for the card issuing fee and other charges arising from card transactions.

The card holder will receive the card and PIN known only to them. The card will be delivered to the card holder at the address of the contracting party's registered office and the PIN will be disclosed by SMS or sent by post to the address of the contracting party's registered office, if such is communicated to the Bank by the card holder upon ordering the card. The Bank shall send the card by ordinary mail. The PIN, if sent by post, shall be sent by registered mail. The Bank will send the card and the PIN in two separate parcels mailed on different days. If the parcel containing the card is returned to the Bank, the Bank will again notify the card holder that a card is available and ask them to collect it. The card must be collected in ninety (90) days of the order. After ninety (90) days the Bank will destroy the card. Immediately after receiving the card, the card holder shall sign it with a permanent pen. The card is not valid unless signed. The contracting party shall bear all the damage and costs arising from abuse of an unsigned card.

When a card is ordered, the Bank will transmit the card holder's personal data (name, surname, mobile phone number, e-mail, etc.) to the external processing centre for the purposes of secure online transactions, payments at points of sale and ATMs, SMS transaction alert for payment card transactions, use of mobile wallet, and other services linked to payment cards.

The card is non-transferrable and may only be used by the card holder. If the authorisation to operate the business account is revoked, the contracting party shall hand over the card to the Bank, and the Bank shall destroy the card and prevent its use.

The Visa business charge card holder agrees to accident insurance for accidental death and permanent disability with the insurance company Sava d.d. for the sum insured of EUR 2,086.46 in case of accidental death and EUR 4,172.92 in case of permanent disability. The General Terms and Conditions for accident insurance of payment card holders are available to card holders at any Bank branch office.

Whenever a card payment is made, the Bank will reduce the available card limit for the total amount of the purchase or payment.

The Bank shall notify the contracting party of liabilities incurred by using the card once per month by way of a card statement. The contracting party is obligated to inspect the monthly statements. If the contracting party is not informed about the liability arising from the purchase or cash withdrawal by a statement within sixty (60)

days, it shall be obliged to notify the Bank thereof. The contracting party shall further be required to immediately notify the Bank of any incorrect debits to the transaction account or any other irregularities.

The contracting party authorises the Bank to debit their transaction account for the liabilities arising from the use of the card. The contracting party undertakes to provide, no later than by the due date, sufficient available balance to settle the liabilities incurred and fees associated with using the card. If the contracting party fails to ensure sufficient balance by the due date to settle the liabilities incurred, including fees and charges, they shall be charged the relevant default interest until sufficient balance has been made available. Default interest will be charged in the amount and using the method stipulated in the Bank's Resolution on interest rates applicable at the time.

The contracting party irrevocably authorises the Bank and gives the Bank a permanent and irrevocable order to use any of the contracting party's balance with the Bank to settle overdue and outstanding obligations arising from the use of the card, irrespective of the agreed maturity.

The Bank will make the limit available on the day when liabilities are paid, in the amount equal to the payment.

3.8.5 Actions to be taken by card holder to protect the business payment card with PIN

The card holder shall use the card in accordance with these General Terms and Conditions and take all reasonable steps to protect the (personal) security elements of the card (PIN number, card number, card expiry date and CVV number).

The card holder must keep the PIN confidential to prevent misuse.

The card holder must memorise the PIN and destroy the PIN notification immediately upon receipt. The card holder can change the PIN at the Bank's ATMs. The changed PIN must contain four randomly selected digits. The PIN must not contain any personal data, such as date of birth, ID card number, etc., or logical sequences (e.g. 1234, 1111, etc.). If the card holder changes the PIN, they shall be responsible for the security of the password they choose. If the card holder forgets the PIN, they can order a new PIN without having to order a new card. The Bank shall charge a fee for issuing a new PIN in accordance with the Fee Schedule. The card holder must keep the card separate from the PIN and must not lend or give the card to anyone for safekeeping or otherwise allow unauthorised persons to use it. The card holder must not disclose the PIN to third parties, write it on a slip or card or otherwise store it with the card.

When entering the PIN at an ATM or POS terminal, the card holder shall shield the keypad with their hand and thereby ensure that third parties cannot learn the number.

The card holder shall not disclose card security elements by telephone, e-mail, SMS, online messaging applications and other unsecured messaging channels, except when requested to do so in the process of making a remote purchase or an online purchase. The card holder shall be alert to e-mails or SMS/MMS messages received with links to websites via the link received in an e-mail or SMS/MMS message, and shall not enter personal data, bank account and payment card details, user names or passwords into forms on such websites. The card holder must also be careful when posting in social media, of receiving e-mails that they have not solicited or requested and of receiving calls asking for personal data, card details, user names and passwords. This information must be kept secure by the card holder and must not be disclosed in such way. In addition, the card holder must not allow remote access to their computer or mobile device to any unauthorised person.
The card holder shall use proper care with the card preventing to the maximum extent the misuse, loss and unauthorised confiscation and thus preventing material loss from being incurred by themselves and the Bank. The card holder must not leave the card unattended (e.g. in the car, office, public area, hotel room, pub, etc.).
Conduct contrary to the provisions of this Chapter of these General Terms and Conditions shall be considered gross negligence on the part of the card holder. The card holder shall be fully liable for any damage resulting from the failure to comply with the practices described in this Chapter.

The card holder shall also comply with any other instructions, warnings or advice of the Bank relating to the use of the card. Information on the safe use of the card is published on the Bank's website, where the Bank provides guidance on the safe use of cards and warns about various online fraud attempts and how to identify them.

3.8.6 Fees and exchange rate

The Bank shall charge the contracting party a fee and charges for card operations in accordance with the Fee Schedule applicable at the time.

If the contracting party withdraws its application between the time the card is ordered and prior to the card being issued, it is required to pay the costs related to issuing the card.

Payment transactions with a Visa business card executed in foreign currency are converted into EUR at the exchange rates of the card system (e.g. Visa Europe) applicable at the time of conversion.

If the card is used to make payments in a currency other than EUR, the card holder shall be debited in EUR, whereby the currency of the transaction shall be converted to EUR as follows: currency of transaction other than EUR shall be converted into USD by applying the buying rate. This amount in USD is then converted into EUR at the selling rate, or the currency of transaction is converted into EUR if the relevant rate is available on the card system exchange rate list. The conversion is made by applying the rates applicable at the time when the card system processes the transaction. The exchange rates applied and the conversion date shall be indicated in the card statement. Due to frequent intraday changes of card system exchange rates, rates applied to transactions made within the same day may differ.

3.8.7 Validity and termination of the right to use the card

The card is valid until the last day of the month indicated on the card. Card holders who comply with these General Terms and Conditions will have their card automatically renewed and sent by mail to the contracting party's address, The card is the property of the Bank, therefore the card holder is required to return the card if so requested by the Bank. The contracting party shall be responsible for all liabilities and costs incurred by using the card until the day when the card is returned to the Bank. The card holder shall be liable to the contracting party for the use of the card.

The Bank may block the card if:

- There are objectively justified reasons associated with the security of the card (e.g. reasons to suspect that the card could be misused or card data stolen, etc.);
- There is a suspicion of the card having been used without authorisation or in a fraudulent manner, or suspicion of card fraud;
- There is a significantly greater risk that the contracting party will not be able to meet its payments, when the use of the card is associated with a loan approved to the payer.

The Bank shall notify the point of sale network through the processing centre of having blocked the card. An employee at a point of sale may retain the card based on the Bank's notification.

The Bank shall notify the client of blocking the card and the reasons therefor in the manner set out in Chapter 3.16.
(Sending notices or informing the user) of these General Terms and Conditions, if possible before the card is blocked, and no later than after blocking, except where such notification is contrary to objectively justified security measures or is prohibited by other regulations. The Bank shall unblock the card or replace it with a new one once the reasons for blocking have ceased.

By signing the agreement under which the Bank issued the card, the contracting party agrees that the Bank may provide the card holder with a new card to replace a payment card already issued.

The contracting party agrees and undertakes to pay to the Bank all liabilities arising from the use of the card also after the closing of the transaction account and of which the Bank was not aware at the time of such closing.

In case of termination of agreement on the issue of a business charge card or death of the card holder, the card shall be terminated as well, irrespective of the expiry date indicated on the card.

The card holder is required to destroy the old card upon its expiry or after receiving the new card.
The card holder shall not use a card that has been cancelled and shall destroy it (cut it through the middle) and return it to the Bank, so that the card number is no longer identifiable.

If the contracting party who is party to a business charge card agreement does not wish to renew the card, they shall inform the Bank thereof at least two (2) months before the expiry of the card, otherwise the Bank shall automatically renew the card by issuing a new card and charge the contracting party the annual card fee in accordance with the Fee Schedule. If the contracting party does not wish to renew the card, they must return it to the Bank.

3.8.8 Lost, stolen or misused business card

The card holder and/or the contracting party shall immediately notify the Bank or the Bank's contact centre or processing centre of the card being destroyed, damaged, lost, stolen or misused. A card can be cancelled by phone via the Bank's contact centre or processing centre 24/7. Telephone numbers are published on the Bank's

website. The telephone number of the processing centre is also indicated on the back of the card. When a card is cancelled due to loss, theft or misuse, the cancelled card will no longer be valid. The card holder can also temporarily block the card themselves in the digital bank.

In the event of theft or misuse or suspected theft or misuse, the card holder or the contracting party shall also report the incident to the nearest police station and deliver the police report to the Bank. The incident shall be reported at the police station at the request of the Bank. The card holder or the contracting party is obliged to provide the Bank with all the necessary information about the circumstances related to the loss, theft or misuse of the card.

Upon reporting a card lost, stolen or misused, the Bank shall issue a new card to the card holder for the same transaction account. The card holder will receive a new PIN as well.

If the card holder finds the card after having reported it lost, stolen or misused, they shall stop using it and must destroy it (cut it through the middle) and return it to the Bank immediately.

3.8.9 Incoming card payments

The card holder may not receive any incoming payments to the card or use the card for purposes other than payments and settlement of liabilities arising from card use. The Bank shall not be liable for these actions of the card holder. If the card holder nonetheless receives incoming payment and has liabilities to the Bank arising from card use within the same billing period, the Bank shall offset both amounts up to the lower of the two, otherwise it shall transfer the incoming payment to the contracting party's transaction account on the maturity date.

3.8.10 Using SMS transaction alert service for card transactions (SMS Alert)

The SMS transaction alert service for card transactions is a method of providing information to card holders by way of text messages to their mobile phones. The service can only be used by the card holder.

The contracting party may subscribe to the SMS transaction alert service for authorised persons. The persons authorised for the contracting party's transaction account may place an order for the service or a request to change data only for their own cards, but shall not have the right to change an order or data previously submitted by the contracting party. The contracting party or a card holder may cancel the SMS transaction alert service for card transactions by way of a written cancellation notice submitted at a Bank branch office or with their bank relationship manager.

If the Bank finds that the contracting party and/or card holder breached the provisions of these General Terms and Conditions, the provisions of the transaction account agreement, or abused the right of service subscription, or caused the Bank damage in any other way, the Bank reserves the right to cancel the SMS transaction alert service.

The service user must provide the Bank with a correct and valid mobile phone number. The service user must immediately notify the Bank of any change of the mobile phone number. The Bank shall send messages to the last known mobile telephone number and shall not be liable if the mobile telephone number is incorrect or invalid. The contracting party shall be solely liable for any consequences arising from any incorrect data given to the Bank.

The service user agrees with the Bank transmitting data on card transactions to the company providing data distribution services. The data distribution company is obligated to protect the data of the service user and use them exclusively for the purpose of providing the service.

The Bank assumes no liability whatsoever for damage caused by the loss or theft of mobile phone or SIM card or other irregularities that arise before the SMS transaction alert service is cancelled.

The service user shall be solely responsible for the security and confidentiality of data stored in the mobile phone.
The Bank shall charge the contracting party a fee and costs for the SMS transaction alert service in accordance with the Fee Schedule applicable at the time.

3.8.11 Complaints

The Bank shall be competent for solving complaints and submitting information related to the use of the card. To file a complaint, the card holder or the contracting party shall contact the Bank and provide relevant documentation. The complaint shall be submitted in writing. The card holder undertakes to remain available for

contact through the contact details they have communicated to the Bank (e-mail, telephone) until receiving a notification that the complaint has been resolved, and to provide the Bank upon request with evidence, statements and documentation necessary to process and resolve the complaint.

If the card holder provides false statements in relation to the complaint, the Bank shall have the right to charge the contracting party the costs of the complaint. Complaints are resolved according to procedures laid down by the rules and instructions of licence holders – Visa card system and the Bank.

The card holder or the contracting party shall notify the Bank of any unauthorised and/or incorrectly executed payment transaction as soon as they become aware that an unauthorised or incorrectly executed payment transaction has occurred, but no later than thirteen (13) months after the date of debiting the transaction account. The card holder shall notify the Bank as soon as possible of any other disputes arising from card use where the card holder was involved in the purchase; it is advised that notification be made within at least eight (8) weeks after a breach has been identified.

The card holder shall resolve any disagreements or errors relating to the quality, execution or delivery of goods and services directly with the point of sale. The card holder shall file a complaint with the Bank only if the disagreement with the point of sale cannot be resolved within eight (8) weeks of the event.

The contracting party shall be required to pay their liabilities to the Bank regardless of any dispute with the point of sale.

3.8.12 Termination of Visa business card agreement

The Visa business card agreement may be terminated by the contracting party or the Bank at any time without cause by giving one (1) month's notice.

The Bank may terminate the agreement without notice and at the same time prohibit further use of the business card and block the card if the contracting party fails to conduct its business in accordance with the agreement and these General Terms and Conditions.

The card holder may be prohibited from further use of the business card by the contracting party, which at the same time requests the Bank to block the business card.

A business card whose further use is prohibited for the above reasons shall be surrendered to the Bank by the card holder or the contracting party.

The financial obligations of the contracting party arising from the use of a business card whose further use is prohibited shall not cease.

3.9 Digital bank (online, electronic and mobile banking)

3.9.1 Use of eBank@Net com electronic bank, Bank@Net com online bank and mBank@Net com mobile bank

Terms and conditions of use

A user may apply for the use of eBank@Net com electronic bank, Bank@Net com online bank and mBank@Net com mobile bank, if the following conditions are met:

- The user has a transaction account opened with the Bank;
- The user submits an "eBank@Net com, Bank@Net com and mBank@Net com Application" form (hereinafter referred to as the application), duly and completely filled out and signed. By signing the application, the user confirms that they are familiar with the provisions of these General Terms and Conditions and the Fee Schedule;
- The user submits a duly and fully completed "Designation of authorised person or revocation of authorisation for eBank@Net com, Bank@Net com and mBank@Net com";
- The user submits a duly and fully completed "Application for Mobile Token Order/Cancellation/Replacement for mBank@Net com and Bank@Net com (if using mBank@Net com mobile banking);
- The user does not have any outstanding and due obligations to the Bank;
- The user is a holder of a qualified digital certificate, which they register with the Bank (if using eBank@Net com electronic bank and Bank@Net com online bank);
- The user has appropriate hardware and software;
- The user has access to the Internet.

The contractual relationship relating to the use of eBank@Net com, Bank@Net com and mBank@Net com is concluded when the Bank and the user sign the application. The Bank may refuse an application to use eBank@Net com, Bank@Net com online and mBank@Net com mobile banking without giving any reason.

The user may not apply for eBank@Net com, Bank@Net com and mBank@Net com if they are already a user of Poslovni Bank@Net online banking services.

The Bank shall enable the user to use each service within five (5) business days from the date of signing the application, and the user may start using the service after installing the relevant software and establishing a connection with the Bank.

eBank@Net com electronic bank and the Bank@Net com online bank may be used with a valid qualified digital certificate issued by the public certification authority Halcom CA. The user may order a qualified digital certificate of issuers for which the Bank provides login service. Bank@Net com online bank can also be used with a user name and a one-time password (from the mBank@Net com mobile bank).

mBank@Net com mobile bank can be used with a mobile token. The user shall receive the components of the activation key for the receipt of the mobile token after signing and submitting the Application for Mobile Token Order/Cancellation/Replacement.

The Bank shall send all information and notifications to the user electronically. Exceptionally, the Bank shall send information to the user in paper form only at the user's specific request and upon payment of the fee set out in the Fee Schedule.

eBank@Net com electronic bank, Bank@Net com online bank and mBank@Net com mobile bank can be used in full functionality or as an archive. Archive use is only available to a user who has opted for such use or who has been assigned such use by the Bank.

Archive use provides the following functionalities:

- **Archive use of eBank@Net com electronic bank:**
  - Overview of transactions in the account and statements up to the date when the archive use of eBank@Net com electronic bank is activated;

- **Archive use of Bank@Net com online bank:**
  - Overview of transactions in the account and statements up to the date when the archive use of Bank@Net com online bank is activated;
  - Viewing of documents up to the date when the archive use of Bank@Net com online bank is activated;
  - Viewing of payment cards, card transactions and card account statements up to the date when the archive use of Bank@Net com online bank is activated.

- **Archive use of mBank@Net com mobile bank:**
  - Overview of transactions in the account and statements up to the date when the archive use of mBank@Net com mobile bank is activated;
  - Viewing of payment cards, card transactions and card account statements up to the date when the archive use of mBank@Net com mobile bank is activated.

If the user closes any transaction account entered in eBank@Net com electronic bank, Bank@Net com online bank or mBank@Net com mobile bank, the closed transaction account shall be deemed to be eligible for archive use of eBank@Net com electronic bank, Bank@Net com online bank or mBank@Net com mobile bank for a period of twelve (12) months from the date of closure of the transaction account. After the expiry of the twelve (12) months, the Bank will de-register the closed transaction account from eBank@Net com electronic bank, Bank@Net com online bank or mBank@Net com mobile bank and the user will no longer be able to use the services in archive use as of the date of de-registration.

Authorised users of eBank@Net com electronic bank, Bank@Net com online bank and mBank@Net com mobile bank

By completing the form "Designation of authorised person or revocation of authorisation for eBank@Net com, Bank@Net com and mBank@Net com", the user authorises at least one natural person to use eBank@Net com, Bank@Net com and mBank@Net com and specifies the scope of their authorisation.

By signing the form referred to in the preceding paragraph, the authorised person agrees to the authorisation and confirms that they are aware of the provisions hereof and that these General Terms and Conditions form an integral part of the contractual relationship relating to the use of eBank@Net com electronic bank, Bank@Net com online bank and mBank@Net com mobile bank.

The user shall determine for each authorised person whether they will access the Bank@Net com online bank with a qualified digital certificate (and which one) and/or with a user name and one-time password (from mBank@Net com mobile bank).

The authorisations of the authorised person must be the same for using mBank@Net com mobile bank as for using Bank@Net com online bank.

For each authorised person who will access Bank@Net com online bank and eBank@Net com electronic bank with a qualified digital certificate, the user must specify the qualified digital certificate used for accessing Bank@Net com online bank and eBank@Net com electronic bank.

Upon the first registration, the authorised person must present the "Written certificate of digital certificate identity" received from the issuer.

The user authorises the Bank to obtain from the certification authority Halcom CA, upon expiry of a particular qualified digital certificate, the number of a new qualified digital certificate issued as a replacement of an expired qualified digital certificate. The user shall arrange for the renewal of the qualified digital certificate.

By granting the authorisation, the user agrees that, from the moment of expiry of the qualified digital certificate, the authorised person may access eBank@Net com electronic bank and Bank@Net com online bank with the new digital certificate, with the scope of the authorisation unchanged.

The user may authorise the authorised person to provide one or more of the following services:

- **in eBank@Net com electronic bank**:
    - Exercising all rights of the user in relation to the use of eBank@Net com electronic bank;
    - Using all services of eBank@Net com electronic bank;
    - Signing payment orders (domestic, cross-border, foreign payment transactions and bulk payments);
    - Sending signed payment orders (domestic, cross-border, foreign payment transactions and bulk payments);
    - Preparing payment orders (domestic, cross-border, foreign payment transactions and bulk payments);
    - Preparing SDD orders;
    - Reviewing data;
    - Exchanging files not directly related to payment transactions;
    - Reviewing, issuing and sending e-documents.

- **in Bank@Net com online bank**:
    - Exercising all rights of the user in relation to the use of Bank@Net com online bank;
    - Using all services of the Bank@Net com online bank;
    - Signing payment orders (domestic, cross-border, foreign payment transactions and bulk payments);
    - Sending signed payment orders (domestic, cross-border, foreign payment transactions and bulk payments);
    - Preparing payment orders (domestic, cross-border, foreign payment transactions and bulk payments);
    - Preparing SDD orders;
    - Reviewing data;
    - Exchanging files not directly related to payment transactions;
    - Reviewing, issuing and sending e-documents;
    - Viewing deposits;
    - Viewing loans;
    - Viewing payment cards and card transactions;
    - Authorisations to subscribe and unsubscribe services.

- **in mBank@Net com mobile bank:**

- Exercising all rights of the user in relation to the use of mBank@Net com mobile bank;
- Using all services of the mBank@Net com mobile bank;
- Signing payment orders (domestic and cross-border payment transactions);
- Sending signed payment orders (domestic and cross-border payment transactions);
- Preparing payment orders (domestic and cross-border payment transactions);
- Reviewing data.

The user may revoke, temporarily block or reduce the scope of the authorisation for a particular authorised person by notifying the Bank.

The Bank shall, no later than by the end of the business day following receipt of the notification referred to in the preceding paragraph, modify or revoke the authorisation for the use of eBank@Net com electronic bank, Bank@Net com online bank and mBank@Net com mobile bank.

If the authorised person's qualified digital certificate or mobile token is revoked or the qualified digital certificate has expired, the authorised person may no longer use eBank@Net com electronic bank, Bank@Net com online bank and mBank@Net com mobile bank with that qualified digital certificate or mobile token. The Bank shall also disregard any actions taken by the authorised person during the validity of the qualified digital certificate or mobile token but received by the Bank after the revocation or after the expiry of the validity of the qualified digital certificate or mobile token.

All actions instructed by the authorised person to the Bank until the change or revocation of the authorisation, the revocation or the expiry of the qualified digital certificate or mobile token shall be considered valid, and the user must therefore also cancel any pending actions (e.g. payment orders in queue).

The user may replace the authorised person's qualified digital certificates.

Using eBank@Net com electronic bank
The Bank shall provide the user with access to a valid version of eBank@Net com electronic bank software by directing the user to the Halcom.com website, where a link to install the software is provided.

The Bank may upgrade the eBank@Net com electronic bank software at any time by notifying the user via eBank@Net com electronic bank. The user undertakes to install the new version of the eBank@Net com electronic bank software within 3 months of receiving the notification.

After the expiry of 3 months from the publication of the new version of the eBank@Net com electronic bank application, the Bank does not guarantee that the previous version of the eBank@Net com electronic bank application will allow the user to perform all the functionalities of eBank@Net com electronic bank, including access to eBank@Net com electronic bank.

Using Bank@Net com online bank and mBank@Net com mobile bank
Use of Bank@Net com is available via the Bank's website.

The mBank@Net com mobile application is installed on the user's mobile device. It is available on the Google Play Store (for mobile devices running Android 8.0 and above) and the App Store (for mobile devices running iOS 14.o).

The Bank endeavours to keep Bank@Net com online bank and mBank@Net com mobile bank available at all times, except when system operation is disrupted or interrupted for reasons beyond the Bank's control (e.g. disruptions and interruptions in the telecommunications network, the Internet, etc.) or to carry out maintenance, upgrades or other necessary work on the system. The Bank shall not be responsible for any disruption or interruption in the operation of the system caused by reasons beyond its control or as a result of maintenance, upgrading or other necessary work on the system. The Bank shall not be responsible for errors occurring during the transmission of data via telecommunications networks.

The Bank reserves the right to temporarily prevent access to Bank@Net com online bank and mBank@Net com mobile bank in case of technical maintenance, upgrading and mandatory download of the new version of mBank@Net com mobile bank. When a new version of mBank@Net com mobile bank is published, the user must download it, otherwise the use of mBank@Net com mobile bank will no longer be possible.

Temporary blocking of the use of the eBank@Net com electronic bank, the Bank@Net com online bank and the mBank@Net com mobile bank

The Bank may temporarily block the use of the eBank@Net com electronic bank, the Bank@Net com online bank and the mBank@Net com mobile bank if there is a suspicion that an unauthorised person has accessed or could access the eBank@Net com electronic bank, the Bank@Net com online bank and/or the mBank@Net com mobile bank.
At any time, the user can submit a request to the Bank to temporarily block the use of the eBank@Net com electronic bank, the Bank@Net com online bank and the mBank@Net com mobile bank or temporary block the use of these services only for an individual authorised person. The Bank shall block the use of the eBank@Net com electronic bank, the Bank@Net com online bank and the mBank@Net com mobile bank by the end of the business day at the latest after receiving the user's notification.

After the use of the eBank@Net com electronic bank, the Bank@Net com online bank and the mBank@Net com mobile bank is temporarily blocked, these services cannot be used during the blockade. All actions of the authorised persons that the Bank received up to the moment of the temporary blocking are considered valid, so the user must also cancel any unexecuted actions (e.g. payment orders waiting in the queue).

If the user does not cancel the blocking of the use of the eBank@Net com electronic bank, the Bank@Net com online bank and the mBank@Net com mobile bank for an individual authorised person within thirty (30) days of its temporary blocking, it shall be deemed that the user has revoked the authorisation of this authorised person.

Performing payment transaction services
The Bank enables the user performance of the following payment transaction services in the eBank@Net com electronic bank, the Bank@Net com online bank and the mBank@Net com mobile bank:

- Issuance of payment orders;
- Monitoring of current balance on the transaction account, obtaining transaction account statements;
- Importing and exporting of data in standardised form for exchange with own applications;
- Receiving and sending of notices;
- Performing cross-border payment transactions;
- Monitoring of executed cross-border payment transactions, transfer of foreign currency, monitoring of payments from abroad;
- Entry and sending of data on the type of inflow (statistics);
- Monitoring of current balances on transaction accounts, monitoring of book balances;
- Monitoring of the daily exchange rate list of the Bank of Slovenia and the corporate exchange rate list of Nova KBM;
- Forwarding of SEPA direct debits;
- Importing and exporting of data for exchange with own applications, receiving and sending of notices.

The payment transaction services listed in the third indent and in the fifth to eleventh indents of the previous paragraph do not apply to the mBank@Net com mobile bank.

The Bank shall execute payment transactions within the time limits and in the manner specified in the contract for opening and managing the transaction account.
In the event of a user complaint due to incorrect execution of a payment transaction, the provisions of these General Terms and Conditions from Chapter 3.14 (Liability and refund for payment transactions) shall apply.

Exchanging files not directly connected with payment transactions
The Bank enables the user to exchange files through the use of the eBank@Net com electronic bank and the Bank@Net com online bank.

For the exchange of each individual type of file, the Bank and the user agree separately through the communication channel in eBank@Net com and Bank@Net com.

Receiving and issuing e-documents
The bank enables receiving e-documents in the eBank@Net com electronic bank, the Bank@Net com online bank and the mBank@Net com mobile bank.

If the user wants to receive e-documents in the eBank@Net com electronic bank, the Bank@Net com online bank and the mBank@Net com mobile bank, they must conclude an agreement with the issuer of the e-document on the method of accepting e-documents and specify one of the transaction accounts as an identification code for routing e-documents.

The bank is not responsible for the correctness of the data contained in the e-document.

The Bank enables issuing of e-documents through the eBank@Net com electronic bank and the Bank@Net com online bank. It is not possible to issue e-documents through the Bank@Net com online bank in the case of using a mobile token.

The Bank will enable the user to forward a package containing an envelope, an e-document and attachments through the eBank@Net com electronic bank and the Bank@Net com online bank, and undertakes to forward this package to the recipient in their electronic bank in an unchanged form.

The user must issue e-documents in accordance with all requirements of the applicable regulations and obtain the consent of the recipient before issuing e-documents.

The user undertakes to accept customer consents received in electronic form via the eBank@Net com electronic bank and the Bank@Net com online bank.

The user must prepare e-documents, attachments and envelopes for consumers in accordance with the e-Slog standard and the Instructions in xml format, with each envelope only containing one e-Slog attachment and one attachment in pdf/a format.

The user must prepare e-documents, attachments and envelopes for private individuals and legal entities in accordance with the Instructions in xml format, with each envelope only containing one e-document and a maximum of two attachments.

The Bank will forward the correctly formatted e-documents to the recipient's electronic bank within two business days at the latest.

The Bank cannot deliver a package to the recipient if it is not prepared in accordance with the applicable e-document exchange standards.

http://www.zbs-giz.si/ If the receiving bank does not deliver the e-document to the recipient in the electronic and online bank, it will inform the user, as the issuer, about this within two business days after receiving the e-document via the eBank@Net com electronic bank and the Bank@Net com online bank.

Ordering services
The Bank enables the user to submit a signed application for the issuance of a documentary letter of credit by the Bank through the Bank@Net com online bank. The authorised person can submit an application for the opening of a documentary letter of credit based on the authorisation of the user.

Replacing mobile token
The bank enables the user to submit an order for the replacement of the mobile token via the Bank@Net com online bank or in person by submitting an application, which each authorised person can do for themselves.

Viewing of documentation
Through the Bank@Net com online bank and the mBank@Net com mobile bank, the Bank enables the user to view the transactions on individual business accounts, view business account statements, e-documents, deposits for which the binding period has not yet expired, view loans for which repayment periods have not yet expired, view card transactions and statements, and view payment cards (valid cards and invalid cards if less than 18 months have passed since the end of validity).
Through the eBank@Net com electronic bank, the Bank enables to the user to view the transactions on individual business accounts, business account statements and e-documents.
Viewing of the documentation is possible for a maximum period of 18 months from the submission of the request for viewing.

Temporary blocking of a deferred payment card
The user of the Bank@Net com online bank and the mBank@Net com mobile bank can temporarily block the use of a Visa business charge card until the blocking is cancelled, and then unblock it themselves.

Remote signing
Through the Bank@Net com online bank and the mBank@Net com mobile bank, the Bank enables the user to sign payment orders that have been prepared and sent for remote signing through the eBank@Net com electronic bank.

One-time password generation
Through the mBank@Net com mobile bank, the Bank enables the user to generate a one-time password for entering the Bank@Net com online bank and a one-time password for confirming payment order bundles in the Bank@Net com online bank.

Biometric login
Biometric login with a fingerprint or facial recognition allows the user to quickly and easily log in and confirm payment orders in the mBank@Net com mobile bank. Biometric login and confirmation of payment orders are intended exclusively for the user of the device, therefore it is the duty of the user to store only their biometric data in their device. If the user keeps the biometric data of other persons on their device, they thereby enables them to access the mBank@Net com mobile bank and perform the services provided by the mBank@Net com mobile bank.

The Bank does not assume responsibility for any damage caused to the user due to misuse resulting from non-compliance with the instructions related to the use of biometric data written in these General Terms and Conditions.

Obligations of the user and authorised persons in connection with the use of the Bank@Net com online bank, the eBank@Net com electronic bank and the mBank@Net com mobile bank
The user undertakes to:

- Comply with the provisions of these General Terms and Conditions and all other instructions received from the Bank, and make all their authorised persons aware of these General Terms and Conditions and the Bank's instructions;
- Protect the software and use it only for procedures directly related to the use of the eBank@Net com electronic bank, the Bank@Net com online bank and the mBank@Net com mobile bank;
- Carefully store the personal security elements, the qualified digital certificate, protect them as a good manager and prevent access to them by unauthorised persons, and prevent their loss, theft and/or misuse, and see that the same careful storage and protection is also provided by their authorised persons;
- Regularly receive and send data;
- Change their personal number (PIN) at the mBank@Net com mobile bank at least once a month;
- Delete the mBank@Net com mobile bank application from the device if they no longer use the device;
- Follow the instructions for use received from the Bank;
- Immediately notify the Bank of any errors or irregularities resulting from incorrect operation or suspected abuse of payment transactions via the eBank@Net com electronic bank, the Bank@Net com online bank and the mBank@Net com mobile bank;
- Immediately notify the Bank of any change or expiry of validity of authorisations;
- Secure access to their smart phone with a password and never leave the smart phone with an active mBank@Net com mobile bank unattended, and log out by clicking on the Logout button each time at the end of using the mBank@Net com mobile bank;
- Be aware of the fact that the e-mail sending system is not a completely reliable and secure way of sending and that it is not always certain that the authorised person will receive e-mails (e.g. due to a full e-mail box, etc.), and waives any claims against the Bank from this title in the event of damage;
- Notify the Bank as soon as they become aware of any unauthorised use or abuse of the Bank@Net com online bank, the eBank@Net com electronic bank or the mBank@Net com mobile bank, or of any loss, theft or abuse of personal security elements, and submit to the Bank a written request to block the Bank@Net com online bank, the eBank@Net com electronic bank and the mBank@Net com mobile bank. The telephone number of the eBank@Net com, Bank@Net com and mBank@Net com administrators is published on the Bank’s website;
- Regularly take care that the qualified digital certificates of their authorised persons are valid by timely arranging for a replacement before the actual expiry; regularly check the received e-documents;
- In the event of the discovery of errors and/or irregularities in the operation of the Bank@Net com online bank, eBank@Net com electronic bank or mBank@Net com mobile bank, take appropriate action with the aim of reducing the extent of the damage.

The user’s authorised person undertakes to:

- Comply with the provisions of these General Terms and Conditions and all other instructions received from the Bank;
- Protect the qualified digital certificate, user name and personal identification number (PIN) with the same due care as stipulated for the user and in a manner that will prevent damage, alienation or abuse;

- Declare, by signing the application for the order of a mobile token, that they are the user of the mobile phone number or email address specified in the application, and agree to receive the registration number and the link to download the mobile application of the mBank@Net com mobile bank. If the authorised person does not receive the registration number and link, they must contact their account manager and request sending of a new registration number, or deregistration of the existing mobile token and registration of a new mobile token;
- Allow the Bank to transmit information about the registration number related to the use of the mBank@Net com mobile bank to the mobile operator through which the authorised person does business, exclusively for the use of the mBank@Net com mobile bank;
- Change the personal identification number (PIN) at least once a month.

The Bank is not liable for any damage caused to the user and their authorised person due to non-compliance with these General Terms and Conditions, the Bank's instructions and applicable regulations, or due to careless handling of authentication elements or enabling the use or disposal of the authentication element by unauthorised persons.
The user agrees that the authorisation with personal security elements is identical to their own handwritten signature, and allows its use as their own signature in all transactions via the Bank@Net com online bank, the eBank@Net com electronic bank and the mBank@Net com mobile bank.

The Bank does not assume any liability for damage or other type of liability for any damage caused by improper and careless handling by the user and/or their authorised person, theft, damage or loss of personal security elements and other irregularities until the blocking of the use of the eBank@Net com electronic bank, the Bank @Net com online bank and the mBank@Net com mobile bank.

The cost of issuing new personal security elements in the event of loss, theft, damage, etc. shall be covered by the user in accordance with the currently valid Fee Schedule.

In case of termination of access to the Bank@Net com online bank and the eBank@Net com electronic bank, the user is obliged to agree with the issuers of e-documents on a new method of sending and to ensure, before the date of termination of the use of the eBank@Net com electronic bank and the Bank@Net com online bank, the timely payment for all e-documents received in the eBank@Net com electronic bank and Bank@Net com online bank before the termination or suspension of the possibility of use.

Cancelling the use of the eBank@Net com electronic bank, the Bank@Net com online bank and the mBank@Net com mobile bank
The Bank and the user may unilaterally terminate the contract for the use of individual services of the eBank@Net com electronic bank, the Bank@Net com online bank and the Bank@Net com mobile bank, or the use of the entire service of the eBank@Net com electronic bank, the Bank@Net com online bank and the mBank@Net com mobile bank with a unilateral statement sent by registered mail with a thirty (30) day notice period.

Before termination, the user must pay the Bank all due obligations incurred when using the eBank@Net com electronic bank, the Bank@Net com online bank and the mBank@Net com mobile bank.

The Bank may terminate the contract without a notice period with a unilateral statement sent by registered mail in the following cases:

- The user no longer has an open transaction account with the Bank or the user's transaction account has been terminated;
- The user has past due payment obligations to the Bank;
- The user unjustifiably interferes with the eBank@Net com electronic bank, the Bank@Net com online bank and the mBank@Net com mobile bank, or the computer system as a whole;
- The user, intentionally or out of gross negligence, causes the eBank@Net com electronic bank, the Bank@Net com online bank and the mBank@Net com mobile bank to malfunction;
- The user violates the provisions of these General Terms and Conditions, the contract concluded or the applicable regulations and continues to do so in spite of a warning by the Bank or fails to eliminate the violations by the deadline set by the Bank;
- The user does not immediately notify the Bank in writing of any change in their data or circumstances that could affect the execution of the contract on the use of the services of the eBank@Net com electronic bank, the Bank@Net com online bank and the mBank@Net com mobile bank;
- Upon the death or loss of business capacity of the user's legal representative or authorised person;
- Initiated insolvency proceedings against the user;
- The existence of a reason for termination based on a judicial or administrative decision or existing legislation.

Upon termination of the contract, the bank shall block the use of the eBank@Net com electronic bank, the Bank@Net com online bank and the mBank@Net com mobile bank. Simultaneously with the termination of the contract, all the user's obligations incurred until then become due.

All payment orders forwarded to the Bank@Net com online bank, the eBank@Net com electronic bank or the mBank@Net com mobile bank before the termination of use will be executed by the Bank if all the conditions under which the Bank guarantees their execution are met.

The user explicitly and irrevocably authorises the Bank and gives it an irrevocable standing order to debit their transaction account for the payment of any overdue obligations. If for any reason it will not be possible to make the payment, the user undertakes to settle all obligations themselves on the basis of the monthly billing of payment transaction services.

Fees

The Bank charges the user fees for using the eBank@Net com electronic bank, the Bank@Net com online bank and the mBank@Net com mobile bank for each individual business transaction account in the amount, within the terms and in the manner specified in the Fee Schedule, from the moment of registration to the moment of deregistration, and includes them in the monthly billing of payment transaction services.

When performing domestic and cross-border payment transactions in EUR or in other currencies, each participating bank charges fees to its user of payment services. Only the code SHARE is allowed on orders regarding the calculation of costs and fees. The code means that the bank's fee is paid by the payer, while all other fees (of the recipient's bank and any intermediary banks) are paid by the payee. If the Bank receives a payment order for a domestic or cross-border payment with the option BEN or OUR, it shall consider such an instruction as unspecified and execute the payment with the option SHARE.

For payments to third countries, the following codes may be used in addition to the code SHARE:

BEN – meaning that the bank's fee and all other fees are paid by the payee. The bank executes such an order by reducing the amount of the payment transaction for its fee;
OUR – meaning that the bank's fee and all other fees (of the recipient's bank and any intermediary banks) are paid by the payer.

The user expressly agrees that the Bank may issue all invoices for banking services to them in electronic form and send them to the eBank@Net com electronic bank, the Bank@Net com online bank and/or the mBank@Net com mobile bank.

The user explicitly and irrevocably authorises the Bank and gives it a standing order to pay the monthly invoices for the payment transaction services when due by debiting the user’s transaction account. If for any reason it will not be possible to make the payment, the user undertakes to settle all obligations themselves on the basis of the monthly billing of payment transaction services.

The Bank charges the user fees for the use of Poslovni Bank@Net in the type, amount, terms and manner specified in the Fee Schedule.

Bank's responsibility in connection with the use of Bank@Net com, eBank@Net com and mBank@Net com

The Bank undertakes to:

- Execute all correctly completed payment orders in a timely manner, in accordance with these General Terms and Conditions and applicable regulations, unless a reason is given for rejecting the payment order;
- Consider all information, facts and circumstances that it has learned about in the course of providing services for the user and in doing business with the user as confidential and a business secret. The Bank shall disclose such information, facts and circumstances only in the cases, scope and manner prescribed by the applicable legislation;
- Protect all personal data of authorised persons and use them exclusively in connection with the use of the eBank@Net com electronic bank, the Bank@Net com online bank and the mBank@Net com mobile bank.

Unless proven otherwise, it is considered that the Bank receives all data that the user successfully transmits through the eBank@Net com electronic bank, the Bank@Net com online bank and the mBank@Net com mobile bank and are marked as “Sent” in the user's archive.

The Bank informs the user of all facts related to the execution of the user's orders via eBank@Net com, Bank@Net com and mBank@Net com.

The Bank is not liable for any damage resulting from the actions or events it cannot control (including but not limited to *force majeure*, strike, decisions and actions of authorities, traffic disruptions, especially telecommunication traffic disruptions and disruptions of traffic intended for computer connection, errors arising in data transfer via telecommunication networks, disabled access to the eBank@Net com electronic bank, the Bank@Net com online bank and the mBank@Net com mobile bank). The Bank is also not liable for any damage caused to the user and/or third parties due to the failure of the eBank@Net com electronic bank, the Bank@Net com online bank and the mBank@Net com mobile bank, or the computer system as a whole, occurring due to careless handling by the user or unauthorised interventions by third parties.

The Bank is only liable for damage resulting from the Bank's intentional conduct or its gross negligence. The Bank's liability for any damage caused is limited only to the amount of ordinary damage. The Bank is not liable for any damage resulting from loss of profit and non-property damage.

In the event of termination of access to the eBank@Net com electronic bank and/or the Bank@Net com online bank, the Bank refuses to forward any newly-arrived e-documents to the user via the eBank@Net com electronic bank and/or the Bank@Net com online bank.

3.9.2 Use of Poslovni Bank@Net

Terms and conditions of use

Poslovni Bank@Net can be used by users with a transaction account opened with the Bank. The user fills in and signs the form “Application form for performing services through Poslovni Bank@Net” (hereinafter: the application form) and the form “Authorisation for performing services through Poslovni Bank@Net” (hereinafter: the authorisation). The Bank notifies the user in writing of the approval or refusal of the user's application within seven (7) business days of receiving the complete application. The Bank may refuse the application without stating the reason. Upon approval of the application, the Bank assigns the user personal security elements (user name and password) that enable them secure performance of services through Poslovni Bank@Net.

The user may authorise one or more natural persons to perform services on the user’s transaction account via Poslovni Bank@Net with a written authorisation. All authorisations must be in writing and signed by hand. If the Bank reasonably doubts the credibility and validity of the authorisation, it may request the submission of a new authorisation and notarisation of the signature of the authorising person on the authorisation. The authorised person may not transfer the authorisation to another person. An authorisation transmitted through Poslovni Bank@Net is valid only for the performance of services through Poslovni Bank@Net. The authorisation remains effective until revoked in writing or until the Bank receives a formal notification on the winding up or an official notice of death of the authorised party, irrespective of any entry of changes of the right of disposal or representation made in any public register, as well as in case bankruptcy proceedings are initiated against the user, if a liquidator is appointed in case of regular dissolution of the user, in case of winding-up or death of the user, and in all other cases set out in applicable law. The Bank takes into account the revocation of the authorisation if the user informs the Bank of the revocation in writing with a duly signed letter or through Poslovni Bank@Net messages.

If the user revokes the authorisation of the authorised person to conduct business through Poslovni Bank@Net and if the authorised person has other valid authorisations to dispose of funds on the user's transaction account, they must confirm the revocation with their signature at the branch that manages the user's transaction account in which the authorised person is still active at the latest on the next business day.

Personal security elements are linked to a specific natural person as the user of electronic banking, and not to the user as the transaction account holder. If the user of Poslovni Bank@Net already uses personal security elements for other applications of the Bank, the latter does not issue new ones. At each login to Poslovni Bank@Net, the user enters personal security elements in accordance with the provisions and instructions received from the Bank.

Execution of payment orders submitted via Poslovni Bank@Net

The provisions of Chapter 3.4 apply to the execution, rejection and cancellation of electronic payment orders submitted via Poslovni Bank@Net. (Execution of payment orders and notification of users) of these General Terms and Conditions.

A payment order submitted via Poslovni Bank@Net is equivalent to a written payment order or a payment order submitted in a bank branch.

Payment orders submitted via Poslovni Bank@Net must be filled out in accordance with the payment transaction standards. The standards are set out in the user instructions of the Bank Association of Slovenia, published on the website www.zbs-giz.si. The user shall be responsible for the accuracy and completeness of data in the payment order. The Bank shall reject payment orders with an execution date in the past, as well as incorrectly and incompletely filled out orders. The Poslovni Bank@Net user sees the rejected orders in the rejected order status in the Poslovni Bank@Net application. It is considered that the Bank did not receive the rejected payment orders and has no obligations towards the user in relation to them.

The user may cancel a payment order, in accordance with the provisions of the chapter “Execution of payment orders and notification of users” of these General Terms and Conditions, based on a written request submitted at a bank branch or by sending a request to cancel a payment order in Poslovni Bank@Net (this applies only to domestic payments in the PBN application).

Rules for using e-documents for the e-document issuer

The Bank enables the user of Poslovni Bank@Net to be included in the e-invoice system and to issue e-documents through Poslovni Bank@Net based on the signature of the Statement of the e-document issuer. The legal relationship between the Bank and the user (issuer) is established with the signing of the Statement of the e-document issuer for inclusion in the e-invoice system.

The issuer can issue the following documents through Poslovni Bank@Net: e-invoice, e-reminder, e-proforma invoice, e-delivery note, e-order form, e-debit note and e-credit note.

Restrictions when sending files with e-documents:

- An individual e-document (envelope of the e-document together with attachments, combined and compressed file) may not exceed 2 MB in size;
- The maximum file size the issuer may import is 200 MB.

The issuer is obliged to observe these restrictions, otherwise the Bank will not process such e-documents.

The recipient of e-documents undertakes to inform the issuer of e-documents and the Bank about any changes related to the receipt of e-documents. The issuer of e-documents undertakes to provide e-documents to the Bank in accordance with these General Terms and Conditions, and to regularly fulfil all obligations arising from this.

The Bank undertakes to accept all e-documents from the issuer, and to process and deliver them to the recipients in accordance with these General Terms and Conditions.

After the exchange of e-documents, the Bank will send a return message to the issuer about delivered and undelivered e-documents in digital form.

The Bank undertakes to make the e-document available to the recipient and to send the bank of the e-document issuer feedback on its delivery or non-delivery to the recipient. The Bank only forwards the received e-document to the recipient and is not responsible for its content.

The Bank will refuse or will not deliver the e-document to the recipient of the e-document if:

- The recipient of the e-document does not have a transaction account open with a bank;
- The recipient of the e-document is not a user of electronic banking;
- The e-document is not issued in accordance with the rules set out in the Manual for e-invoice exchange, published on the BAS website.

Archival use

Poslovni Bank@Net can be used in its full functionality or as archival use. In archival use, the user agrees and undertakes to use only the following functionalities:

- Viewing of the user's transaction account transactions and statements until the day when it is determined that they stop using Poslovni Bank@Net in full functionality; and
- Viewing of payment cards, card transactions and card account statements until the day when it is determined that they stop using Poslovni Bank@Net in full functionality.

Obligations of the user in connection with the use of Poslovni Bank@Net

The user and authorised persons undertake to comply with these General Terms and Conditions and all other instructions received from the Bank or published on the Bank's website in their business operations.

The user agrees that the authorisation with personal security elements is identical to their own handwritten signature, and allows its use as their own signature in all transactions via Poslovni Bank@Neta.

The user and authorised persons undertake to carefully protect personal security elements and not to communicate or hand them over to any other unauthorised person (this also applies to a qualified digital certificate). The user shall assume all responsibility for any damage resulting from non-compliance with these General Terms and Conditions, instructions and regulations and careless handling of authentication elements (including but not limited to allowing access to authentication elements to unauthorised persons), regardless of whether such conduct occurred on the part of the user or an authorised person.

The user undertakes to report any loss, theft or abuse of personal security elements to the Bank or the administrator of electronic banking as soon as they become aware of it. The telephone number of the Poslovni Bank@Net administrators is published on the Bank's website. The Bank shall accept such reports 24/7. The cost of issuing new personal security elements in the event of loss, theft, damage, etc. shall be covered by the user in accordance with the currently valid Fee Schedule.

The user also undertakes to immediately notify the Bank of any error or irregularity that may be the result of incorrect functioning or suspected abuse of financial payment transactions via Poslovni Bank@Net.
The Bank does not assume any financial or other type of responsibility for any damage caused by theft, damage or loss of personal security elements and other irregularities until the blocking of the use of Poslovni Bank@Net is implemented. The Bank does also not assume any responsibility for any damage caused by improper and careless conduct of the user or their authorised persons.

Obligations of the Bank in connection with the use of Poslovni Bank@Net
The Bank reserves the right to preventively block the use of Poslovni Bank@Net or a payment transaction through Poslovni Bank@Net in the event that it takes business security measures due to the existence of suspicion that there could be abuse or theft of personal security elements or the existence of suspicion of an unauthorised or fraudulent use, or for other security reasons.

The Bank informs the user about the preventive blocking in writing by mail, via Poslovni Bank@Net or in another way customary for the Bank. To unblock the use of Poslovni Bank@Net or a blocked payment transaction, the user contacts the bank branch.

The Bank is not liable for any damage resulting from the actions or events it cannot control (including but not limited to *force majeure*, strike, decisions and actions of authorities, traffic disruptions, especially telecommunication traffic disruptions and disruptions of traffic intended for computer connection, errors arising in data transfer via telecommunication networks, disabled access to Poslovni Bank@Net). The Bank is also not liable for any damage caused to the user and/or third parties as a result of improper conduct or incorrect user data entry in Poslovni Bank@Net, or due to failure of Poslovni Bank@Net or the computer system as a whole, occurring due to careless handling by the user or unauthorised interventions by third parties.

The Bank is only liable for damage resulting from the Bank's intentional conduct or its gross negligence. The Bank's liability for any damage caused is limited only to the amount of ordinary damage. The Bank is not liable for any damage resulting from loss of profit and non-property damage.

Fees
The Bank charges the user fees for the use of Poslovni Bank@Net for each individual business transaction account in the amount, terms and manner specified in the currently applicable Fee Schedule.

Cancelling the use of Poslovni Bank@Net
The user may cancel the use of Poslovni Bank@Net in writing by submitting a request at any branch of the Bank. The cancellation takes effect within 2 hours of submitting the written request if the request is submitted during the Bank's working hours (except Saturdays and Sundays). Prior to cancellation, the user must settle all their obligations toward the Bank resulting from the use of Poslovni Bank@Net.

For a user of Poslovni Bank@Net that is also a user of eBank@Net com, Bank@Net com and mBank@Net com, the Bank may at any time unilaterally disable the use of Poslovni Bank@Net in full functionality and enable the use of Poslovni Bank@Net only for archival purposes, unless the user and the Bank agree otherwise.

The Bank may unilaterally terminate the use of Poslovni Bank@Net at any time with a general two-month notice period.

Notwithstanding the above, the Bank may terminate the use of Poslovni Bank@Net with immediate effect if it finds:

- That the user acted in violation of the Transaction Account Opening and Management Agreement, the provisions of these General Terms and Conditions, and the applicable regulations;
- That the user abused the rights or violated operations through Poslovni Bank@Net;
- That the user's transaction account is terminated;
- Upon the death or loss of business capacity of the user, the user's legal representative or authorised person;
- That insolvency proceedings have been initiated against the user;
- that there are grounds for termination based on a court or administrative decision or existing legislation, including restrictive measures.

The user expressly and irrevocably authorises the Bank and gives it a standing order to debit the transaction account specified by the user in the application form for the payment of all due obligations arising from operations using Poslovni Bank@Net. If for any reason it will not be possible to make the payment to the debit of the funds on the user's transaction account, the user undertakes to settle all obligations themselves on the basis of the monthly billing of payment transaction services.

3.10 Using the mobile wallet of the Bank and other providers

3.10.1 Basic information

A mobile wallet is an application of the Bank or other provider that a user can install on a mobile device. It is intended for storing cards and performing contactless payment services with them via NFC technology, and some also have additional functionalities, such as storing loyalty cards and providing other payment services.

The Bank is not responsible for any disruptions or malfunctions of the mobile wallets of other providers. The Bank is also not responsible for any upgrades or impossibility of access or for non-acceptance of the card in digital form at the point of sale. The card holder decides independently whether to accept the terms and conditions of the mobile wallet provided by a particular mobile wallet provider. The card holder shall obtain answers to any questions about the functioning of the mobile wallet from the mobile wallet provider.
Each mobile wallet provider may have its own general terms and conditions, which the card holder accepts before starting to use the mobile wallet.

3.10.2 Terms and conditions of use

To install and use a mobile wallet, the user must secure access to the Internet and a suitable mobile device.

To obtain the right to use all the functionalities of a mobile wallet, one must register and meet the following conditions:
Use a personal account;
Use one of the payment cards issued by the Bank in the user's name;
Have a smart phone or tablet:
with the corresponding operating system specified on the website,
with the possibility of using NFC (Android) and camera (Android and iOS),
with the mobile device lock function activated.

If the user turns off the NFC (Android) function or the mobile device lock function, they will not be able to use the mobile wallet until they turn the functions back on.

The mobile wallet enables the following payment transaction methods:

- Android operation system users:
  - Payment with the selected payment card issued by the Bank in the user's name;
    - If the user only unlocks the mobile device and brings it close to the POS terminal, the default card will be used to execute the payment transaction;
    - If the user enters the mobile wallet and selects one of the cards registered in the mobile wallet to execute the payment transaction, the selected payment instrument will be used to execute the payment transaction;
    - If the device is brought close to a contactless ATM, only the default payment card will be able to be used; if the card is not default, the user can make a withdrawal only by selecting a card in the mobile wallet;

- execution of instant Flik payments;

- iOS operation system users:
  - Instant Flik payments are enabled;
- confirmation of online payments made with cards.

3.10.3 Adding a payment card to the mobile wallet

The card holder can add their card issued by the Bank to the mobile wallet as instructed by the mobile wallet provider. In the event that the Bank issues a new or replacement card, the card holder must reload the new card into the mobile wallet. The holder can load the card in multiple mobile wallets or on multiple devices. The card holder can only add the card to the mobile wallets of other providers with which the Bank has a contractual relationship. The list of these can be found on the Bank's website.
In the case of using mobile wallets of other providers, the card holder must check whether they meet all the required conditions that other providers specify for the use of mobile wallets.

The Bank may refuse or prevent the addition of cards to the mobile wallet for several reasons, such as violation of the general terms and conditions governing the relationship with the card holder or if the card is cancelled, invalid, blocked or terminated.
The Bank is not responsible for cases where the mobile wallet provider refuses to add a card to the mobile wallet.

3.10.4 Provision of payment services

With the mobile wallet, the user can:

- Issue a payment order for the transfer of funds to the credit of the payment account of the point of sale holder that is marked with a contactless payment symbol and a Visa sticker for Visa payment cards;
- Order a payment transaction at a POS terminal, withdraw or deposit cash, or check the transaction account balance at a contactless ATM in the following way:
- the user brings the mobile device close to the POS terminal or contactless ATM. If confirmation of the transaction is required, the user enters the PIN of the card at the POS terminal or contactless ATM or follows the instructions on the POS terminal or ATM and confirms the transaction accordingly on their mobile device; the user issues a payment order for the transfer of funds and submits a request for receiving funds via Flik.

The provisions of Chapter 3.4 (Execution of payment orders and notification of users) of these General Terms and Conditions also apply to the execution of payment orders via a mobile wallet.

3.10.5 User obligations and mobile wallet security

The mobile wallet user undertakes to:

- Carefully protect the mobile device and keep its security elements, handle it like a good manager in order to prevent theft, loss or abuse of the mobile device, and not to make the mobile device available to third parties. They shall be responsible for any damage caused by third parties using their mobile device;
- Secure access to their mobile device with security elements and not leave the mobile device unattended with an activated mobile wallet;
- Remove the mobile wallet from the mobile phone upon cessation of use of the mobile device on which the mobile wallet is installed;
- Ensure that the device on which the mobile wallet is installed is protected from viruses and hacks. The Bank recommends that the user installs quality anti-malware software on the device, which is frequently updated automatically, activates a firewall on the device and regularly updates the operating system and other software installed on the device. The user is responsible for selecting, using and maintaining the security system to protect the mobile device on which the mobile wallet is installed and shall be fully liable for any damage incurred by them or the Bank as a result of malicious software on their mobile device;
- Not download applications to the mobile device other than from the Google Play or App Store and applications that may interfere with or damage the mobile wallet. If they cause damage out of negligence, they shall be fully liable for it;
- Regularly monitor the notices in the Google Play and App Store mobile stores, and download new versions of the mobile wallet;
- Regularly monitor the Bank's and the mobile wallet provider's notices regarding the use of the service on the Bank's website or in the mobile wallet;

- Inform the Bank of any incorrect functioning;
- Notify the Bank of any change in their mobile phone number;
- use the mobile wallet in accordance with the provisions of these General Terms and Conditions or the general terms and conditions of the mobile wallet provider.

The mobile wallet user shall be solely responsible for the security and confidentiality of data stored on the mobile device. The Bank does not assume any responsibility for any abuse of data stored on the mobile device. The Bank does not assume any responsibility for any damage caused by the mobile wallet user's improper and careless handling of the mobile wallet or mobile device.

3.10.6 Lost, stolen or misused mobile device

The user of the mobile wallet undertakes to immediately report the loss, theft or misuse of the mobile device on which the mDenarnic@ mobile wallet is installed, with the aim of deregistering the mDenarnic@ mobile wallet, to the phone number of the Bank's contact centre or the phone number of the processing centre, or notify the Bank in person or in writing. The telephone numbers of the Bank's contact centre and service centre are published on the Bank's website.

If the user loses their mobile device on which their mobile wallet is loaded and payment cards registered, or the device is stolen, the user can still make payments with the physical payment card. If the card holder loses their physical card or the card is stolen, the card registered in the mobile wallet also ceases to function after its blocking.

3.10.7 Responsibility of the Bank in relation to the mobile wallet

The Bank undertakes to:

- Perform its obligations in accordance with these General Terms and Conditions;
- Notify the user of any amendment or supplement to these General Terms and Conditions and the Fee Schedule, and publish the changes on the Bank's website and in its branches in accordance with the provisions of the General Terms and Conditions;
- Inform the user about any novelties in relation to the mDenarnic@ mobile wallet, but not also about novelties related to mobile wallets of other providers;
- Ensure that the mDenarnic@ mobile wallet is accessible at all times, except when access to the mDenarnic@ mobile wallet is difficult or impossible due to reasons beyond its control, or when the operation of the system is disrupted or interrupted due to maintenance, upgrades, etc.

The Bank is not responsible for disruptions and interruptions in the telecommunications network, for errors occurring during data transmission via telecommunications networks, or for disabled access to the mobile wallet for reasons beyond the Bank's control (and also not during maintenance, upgrading or other necessary work on the system), or for outages due to *force majeure* or causes beyond the Bank's control.

3.10.8 Fees

The Bank charges the mobile user the costs and fees in accordance with the Fee Schedule applicable at the time. The use of a mobile wallet may result in mobile data transfer costs for the user.
Other mobile wallet providers may charge their own fees for using the mobile wallet.

3.11 Transaction account overdraft

3.11.1 Extraordinary transaction account overdraft

Extraordinary transaction account overdraft means the disposal with funds on the transaction account in excess of the current balance on the transaction account (permitted negative balance) based on the concluded loan agreement.

The Bank approves an extraordinary overdraft if the Bank's conditions are met in accordance with the Bank's lending policy. In the event of termination of the user's transaction account, the Bank prohibits the user from using the extraordinary overdraft on the transaction account and terminates the loan agreement in accordance with the provisions of the loan agreement. The user is obliged to return to the Bank the amount of the used extraordinary overdraft on the transaction account within the deadline set by the Bank.

The extraordinary overdraft is used in such a way that the user executes payment orders to the debit of the transaction account.

The user expressly and irrevocably agrees that the Bank is entitled to look into the SISBIZ/SISBON credit risk management information system of banks for the purpose of establishing and maintaining a business relationship with the user.

3.11.2 Automatic transaction account overdraft

Automatic transaction account overdraft means the permitted disposal with funds in excess of the positive balance on the transaction account (permitted negative balance), provided that the user meets the Bank's terms and conditions. The amount of the automatic overdraft is determined in accordance with the Bank's lending policy, depending on the bundle and segment of the user, and amounts to EUR 500.00 for sole proprietors and self-employed professionals, and EUR 1000.00 for legal entities. Non-profit institutions that provide services for households (association) are not eligible for automatic overdraft.

The Bank may unilaterally change the amount of the approved automatic overdraft at any time or disable its use, informing the user of this in the manner specified in these General Terms and Conditions. If the user does not agree with the overdraft amount, they may agree on its change, unless the Bank changed the overdraft amount in accordance with its business policy. In the event of cancellation of the automatic overdraft, the user is obliged to immediately reimburse the Bank for the amount of the used automatic overdraft. In the event of cancellation of the automatic overdraft by the Bank, the Bank may, at its own discretion, restore the overdraft to the user, with which the user expressly agrees.

As part of the Smart Business bundle, the Bank may approve an automatic overdraft for a period of twelve (12) months, with the possibility of automatic extension.

The Bank and the user shall agree on the terms and conditions of using the automatic overdraft with the agreement on opening and maintaining a transaction account, or with the Agreement on accepting the bundle offer on the transaction account.

The automatic overdraft is used for the performance of payment services to the debit of the user's transaction account.

The Bank shall calculate interest for the automatic overdraft in accordance with the Resolution on interest rates applicable at the time. The user shall settle the interest monthly on the due date as specified on the monthly invoice for the payment transaction services.

The user expressly and irrevocably agrees that the Bank is entitled to look into the SISBIZ/SISBON credit risk management information system of banks for the purpose of establishing and maintaining a business relationship with the user.

If the user wishes to have a higher automatic overdraft than they are entitled to within the bundle, their request shall be treated as an application for the approval of an extraordinary overdraft, with the Bank assessing whether the conditions for an extraordinary overdraft are met. If the user has an approved extraordinary overdraft on the transaction account, they cannot use the automatic overdraft at the same time. The automatic overdraft on the transaction account is restored after the expiry of the extraordinary overdraft on the transaction account if all the required conditions are met.

3.12 Bundle offer

The Bank enables the use of bundle services if the user and the Bank so agree. The Bank and the user enter into an Agreement on accepting the bundle offer on the transaction account. The bank has the right to withdraw or change any of the services of an individual bundle at its own discretion. The user shall be informed about this in the manner specified in these General Terms and Conditions.
The single fee for the use of the services in the bundle may change if the Fee Schedule is changed. The general terms and conditions applicable at the time, available on the Bank's website, shall apply to individual services in the bundle.
Automatic renewal or special issuance of a debit card is not included in an individual bundle. If the user already has a debit card, the Bank shall issue a free debit card to them as part of the bundle at their express request or, if the benefit is used for the first time, when the validity of the existing card expires.
The Bank, at its own discretion, approves or rejects the user's application for the allocation of a bundle without giving a reason.

3.12.1 Smart Business bundle

The "Smart Business" bundle, which is intended for sole proprietors, self-employed professionals and associations, includes the following services for a single monthly fee set in the Fee Schedule applicable at the time:

- Transaction account management;
- Use of business online, electronic and mobile banking;
- Issuance of Visa debit cards;
- Security SMS notifications on transactions made with Visa business debit cards;
- Membership fee for all Visa business charge cards issued on this business account;
- Security SMS notifications for all Visa business charge cards issued on this business account;
- Five incoming domestic/cross-border transactions;
- Automatic transaction account overdraft without origination fees; not available to non-profit institutions that provide services to households (associations), which are not eligible for automatic overdraft;
- Rental fee on new POS terminal leases (for 3 months).

The "Smart Business" bundle, which is intended for legal entities, includes the following services for a single monthly fee set in the Fee Schedule applicable at the time:

- Transaction account management;
- Use of business online, electronic and mobile banking;
- Issuance of Visa business debit cards and business prepaid cards;
- Membership fee for Visa business charge cards;
- Security SMS notifications on transactions made with Visa business debit cards, Visa business prepaid cards and Visa business charge cards;
- Five internal outgoing domestic/cross-border online/electronic/mobile bank transactions;
- Fifteen incoming domestic/cross-border transactions;
- Automatic transaction account overdraft without origination fees; not available to non-profit institutions that provide services to households (associations), which are not eligible for automatic overdraft;
- Rental fee on new POS terminal leases (for 3 months).

The Smart Business bundle for legal entities is also available to self-employed professionals and sole proprietors under special terms and conditions specified by the Bank.

3.12.2 Smart Smart bundle

The "Smart Smart" bundle, which is intended for sole proprietors and self-employed professionals, includes the following services for a single monthly fee set in the Fee Schedule applicable at the time:

- Transaction account management;
- Use of business online, electronic and mobile banking;
- Issuance of Visa debit cards.

3.13 Special Debits to Transaction Account

3.13.1 Cashing of domiciled bills issued or accepted by the user

In accordance with the regulations governing payment services and collection of bills in banks, and within available balance on the transaction account, the Bank will debit the user's transaction account based on a submitted bill, if the following conditions are met:

- Such a bill contains a clause making it payable at the Bank (domiciliary clause);
- The user's transaction account is not frozen due to enforcement, enforcement draft or outstanding liabilities to the Bank;
- No bankruptcy proceedings have been initiated against the user, and
- The conditions for payment of the bill are met in accordance with the relevant legislation.

If the Bank receives a bill of exchange by 12:30 on a business day, the bill will be processed on the same day. If the Bank receives a bill of exchange after 12:30 on a business day, it shall be understood that the Bank received the bill on the next business day.

The Bank cashes bills of exchanged at a single, centralised location. It shall be understood that the Bank received the bill at the moment when the bill was delivered to the unit that cashes bills.

The bill shall be understood to contain an irrevocable authorisation of the user to the bill holder to request payment on the basis of a domiciled bill and order the execution of a payment transaction to the debit of the user's balance on the transaction account opened with the Bank, and the user's irrevocable consent to their bank to carry out the payment transaction ordered by the holder of the bill to the debit of the user's balance on the transaction account opened with the bank.

3.13.2 Enforcement against transaction account balances and securing of claims with these balances

In the event that the Bank receives a decision on enforcement, securing of claims or other coercive intervention against the funds on the user's transaction account issued by a court or other authority competent for enforcement and securing of claims, the Bank shall prevent the user from disposing of the funds on the transaction account, and proceed in accordance with the decision of the court or other authority and the applicable legislation.

In doing so, the Bank shall comply with the regulations governing enforcement and securing of claims, and regulations governing payment services. The Bank shall have no duty to verify the relationship between the transaction account user and the person designated as the creditor in the decision on enforcement or securing of claim.

The Bank charges a fee for the acceptance and execution of the decision in accordance with the Fee Schedule applicable at the time.

3.13.3 Cashing of enforcement drafts

The Bank settles the obligations from an enforcement draft in accordance with the regulations governing the prevention of payment delays.
An enforcement draft can only be issued for payment under contracts under which one party undertakes to deliver goods or perform a service, and the other party undertakes to fulfil a monetary obligation. An enforcement draft cannot be issued for the payment of debt arising from a financial transaction (credit agreement, loan agreement, factoring, etc.).

Only undertakings (including sole proprietors) and public authorities can act as a party (creditor and debtor) to an enforcement draft.

3.14 Liability and refund for payment transactions

3.14.1 Liability of the Bank for unauthorised payment transaction

The Bank is liable to the user for having executed a transaction without the user's consent to execute (unauthorised payment transaction). If the Bank is liable for the execution of an unauthorised payment transaction, it shall refund the user the sum of the unauthorised payment transaction immediately and in any case not later than by the end of the next business day after the user noticed the transaction or was notified thereof, unless the Bank reasonably suspects that the transaction is a case of fraud or scam, and informs the Bank of Slovenia in writing of the reasons for the suspicion, and in case of suspicion that a criminal act prosecuted *ex officio* has been committed also the police or the state prosecutor's office.

If an unauthorised payment transaction was debited to the user's payment account, the Bank shall re-set the balance of the user's payment account to the balance as it would have been had the unauthorised payment transaction not been executed and ensure that the user's payment account is not credited later than the date on which the amount was debited. In case the Bank is liable for the execution of an unauthorised payment transaction, it shall also refund the user all the fees charged and the interest to which the user is entitled with respect to the execution of the unauthorised payment transaction.

The Bank shall not be held liable for refunding the sums of unauthorised payment transactions:

- If an unauthorised payment transaction was executed due exceptional and unforeseeable circumstances the Bank could not control or where the impact of such circumstances would arise despite the Bank's best efforts;
- If the user is responsible for the unauthorised payment transaction (including but not limited to cases where the unauthorised payment transaction is the result of a stolen or lost payment instrument, misuse of the payment instrument, the user's fraud or scam, or because the user intentionally or due to gross negligence failed to fulfil one or more obligations in in relation to the payment instrument in accordance with these General Terms and Conditions);
- If the obligation to execute a payment transaction results from other regulations binding for the Bank;
- If the user submitted to the Bank a counterfeit or modified payment order;

- In the amount from the following paragraph covered by the user if the execution of an unauthorised payment transaction is the result of the use of a stolen or lost payment instrument or a payment instrument that was misused (if the user has not protected the personal security elements of the payment instrument);
- If the user failed to, immediately and without delay, notify the Bank of any unauthorised payment transaction when determining that such a transaction has been made, or notify the Bank no later than in thirteen (13) months after the date of credit or debit.

The user shall bear the loss of the unauthorised payment transaction in the sum of up to EUR 50.00 if the unauthorised payment transaction that caused the loss resulted from the use of a stolen or lost payment instrument or misuse of the payment instrument. The user shall bear the full total loss of the unauthorised payment transaction if the unauthorised payment transaction was executed as a result of fraud or scam committed by the user, or if the user, by wilful wrongdoing or gross negligence, failed to fulfil their obligations with regard to the payment instrument.

Notwithstanding the previous paragraph, the Bank must reimburse the user for the entire loss of the amount of the unauthorised payment transaction if the Bank did not provide the means to inform about the lost, stolen or misused payment instrument, or the unauthorised payment transaction occurs after the receipt of the notification from the user that the card was lost, stolen or misused. The Bank shall be released from liability under this paragraph if the damage is the result of the user's fraud or scam.

3.14.2 The Bank's liability for non-execution, incorrect execution or late execution of a payment transaction

If the Bank is liable for the non-execution and/or incorrect execution and/or a late execution of the payment transaction, it shall refund the user without undue delay the sum of the non-executed or incorrectly executed payment transaction or, if the payment transaction was debited to the user’s account, re-set the balance of the user’s payment account to the balance as it would have been had the payment transaction not been executed incorrectly, including any fees charged. The user is entitled to interest only in the case of an incorrectly executed payment transaction for which the Bank is liable.

If the Bank proves that the sum of the payment transaction was credited to the account of the payee’s payment service provider in accordance with Article 127 of the Payment Services, Services of Issuing Electronic Money and Payment Systems Act, the payee’s payment service provider is liable to the payee for the correct execution of the payment transaction in accordance with Articles 129 and 130 of the cited Act and shall immediately make the sum of the incorrectly executed payment transaction available to the payee or, if the payment transaction is credited to the payee’s payment account, credit the appropriate sum to the payee’s payment account. The value date of crediting the payee’s payment account shall not be later than the date when the sum should have been credited had the payment transaction been executed correctly.

The Bank shall be released from liability for the refund of non-executed or incorrectly or late executed payment transactions:

- If the non-execution, incorrect or late execution of payment transactions was caused by exceptional and unforeseen circumstances that the Bank could not avoid or prevent;
- If the non-execution, incorrect or late execution of payment transactions is the result of the Bank performing obligations arising from other regulations binding for the Bank;
- If the user failed to notify the Bank immediately and without undue delay of the non-executed, incorrectly executed or late payment transaction after finding out about such a transaction and by no later than thirteen (13) months after the credit or debit date.

3.14.3 Liability for the use of a unique identifier

If the user provides the Bank with an incorrect payee’s unique identifier on the payment order or any other incorrect essential element of the payment order, the Bank shall not be liable towards the user for the wrong execution of the payment order.

If the user, in addition to the unique identifier or other data on the payee requested by the Bank for the execution of the payment order, provides the Bank with other information as well, the Bank shall be responsible only for the execution of the payment transaction based on the unique identifier delivered by the user.

If the Bank has executed a payment transaction based on an incorrect unique identifier provided by the user, the Bank shall, within reasonable limits, strive to recover the amount of the payment transaction executed.

The user shall be responsible for the accuracy and completeness of data on the payment order. The Bank shall not be liable for any damage incurred by the user as a result of the execution of falsified or modified payment orders.

3.15 Repayment of overdue liabilities to the Bank

In the event that the user does not fulfil any of their financial liabilities to the Bank on time and in full, the user expressly and unconditionally allows the Bank and expressly and irrevocably authorises it to pay and settle its overdue claims against the user, without a special additional order, with funds from any of the user's credit balance at the Bank, including any funds on the user's transaction account and inflows to this account, as well as other deposited and tied funds of the user at the Bank. The relevant authorisation to the Bank is deemed to be an irrevocable payment order of the user in accordance with the provisions of the payment services and systems act applicable at the time.

3.16 Notifying the Bank on changes

The user undertakes to notify the Bank immediately, and at the latest within five (5) days from the date of the change, of all status changes, changes of legal representatives or authorised persons, and other changes necessary for the implementation of the contractual relationship with the Bank. The Bank shall not be liable for any damage arising from failure to comply with the obligations regarding the notification of changes.

Using data from the Slovenian Corporate Register, the Bank shall have the right to change data on the user in its records, such as the name of the user, corporate address, legal representative, etc., to which the user expressly consents.

3.17 Notification on payment transactions

The Bank shall notify the user in writing on the balance and transactions on the transaction account and on any changes at least once a month by mail, by way of a notification collected in person at a Bank unit, or through electronic banking, or by any other means of communication commonly used in banking. If the user is also a user of digital banking, the Bank shall notify the user on the balance and transactions on the transaction account and on any changes via digital channels. In case of written notification sent by mail, the notification shall be deemed to have been served correctly if it is sent to the last known address of the user kept in the Bank's records. If the parcel returns to the Bank as “address unknown/moved” or due to any other similar cause that makes it impossible to deliver the mail, the Bank shall not be required to seek the user’s new address; it can, however, stop sending notifications to this address and modify the notification method to any other method used by the Bank that is the most appropriate by discretion of the Bank.

If the user’s preferred notification method is the e-Notification portal, it shall be understood that the Bank uses the last communicated email address for notifications. If the Bank receives an “undelivered email” message when sending the notification to this address (e.g. invalid or incorrect email address), and the user fails to communicate to the Bank the correct email address, the Bank, in order to ensure due distribution of messages, will modify the notification method to any other method used by the Bank that is the most appropriate by discretion of the Bank.

If the user selected to collect account statements in person, they shall collect them monthly in the Bank. The user shall be responsible for all consequences associated with the failure to collect account statements within the period referred to in the preceding paragraph of this Point.

The Bank provides the user in the account statement with information on executed transactions, such as: information on the payer and payee (account no., name or company name), information on the transaction (amount, currency, purpose (in case of using unstructured credit reference), purpose code, complaint data, reference code, identification numbers, date of entry, expiry date, and reference date).

According to the SEPA DD rules, the payer’s bank shall include the following SEPA DD information in the account statement: designation of the scheme, payee’s name, payee’s identifier, unique authorisation reference number, SEPA DD amount, and a notification of the payee to the payer regarding the payment (if submitted by the payee).

By request of the user, the Bank may always provide the user with all the information on the payment transaction the Bank had received.

3.18 Sending notices or informing the user

If the user is also a user of the digital bank, the user expressly agrees that the Bank may send them all correspondence for which these General Terms and Conditions do not provide for otherwise via the digital bank or to the last communicated email address.

In case of correspondence sent by mail, the notification shall be deemed to have been served correctly if it is sent to the last known address of the user kept in the Bank's records. If the parcel returns to the Bank as “address unknown/moved” or due to any other similar cause that makes it impossible to deliver the mail, the Bank shall not be required to seek the account holder’s new address; it can, however, stop sending notifications to this address.

The user expressly agrees that the Bank may also communicate with the user by sending SMSs to the telephone number the user communicated to the Bank.

3.19 Interest Rates, Fees and Exchange Rates

3.19.1 Transaction account interest rates

The Bank pays interest on funds held in the transaction account at the interest rate for demand deposits, in accordance with the Decision on interest rates of the Bank. The Bank charges interest under the Transaction Account Opening and Management Agreement in the linear method by considering the actual number of days in a month and the actual number of days in a year (365/366), which applies to corporate accounts, or by considering a 360-day year, which applies to accounts held by other entities. In determining the start and end dates of the interest accrual period, the Bank considers the first day after the Transaction Account Opening and Management Agreement has been entered into, however, not the last day.

Any changes in interest rates become effective immediately and without prior notification of the user. The user shall be informed about a change in the interest rate on the transaction account in such a way that the Bank publishes the change in the interest rate on its website or in another way suitable for banking operations, unless the change in the interest rate is in favour of the user.

Interest on the transaction account is capitalised monthly upon calculation. The Bank shall notify the user of the amount of capitalised interest in the account statement.

The Bank charges interest on unauthorised debit balance on the transaction account in accordance with the Fee Schedule.

3.19.2 Transaction account fees

The Bank charges fees for payment services, services relating to the use of the transaction account, and other services the Bank provides under the Transaction Account Opening and Management Agreement or other agreement entered into with the user and in accordance with these General Terms and Conditions. The Bank charges fees in the amount, within timelines and in the method set out in the Fee Schedule applicable at the time. The user undertakes to pay the fees charged by the Bank based on the Transaction Account Opening and Management Agreement or other agreement entered into with the Bank and in accordance with these General Terms and Conditions in the manner agreed on in the agreement with the Bank. If the selected method is to debit the fee to the user’s transaction account, it shall be understood that by signing the Transaction Account Opening and Management Agreement the user expressly gives the Bank a permanent and irrevocable order, and irrevocably authorises the Bank to debit such fees to the user’s transaction account. If the parties agreed that the Bank shall issue an invoice for such fees, the user undertakes to settle all obligations within the timeline and in the manner specified in the issued invoice. This does not exclude the right of the Bank set out in Chapter 3.15. (Repayment of overdue liabilities to the Bank) of these General Terms and Conditions.

The user shall pay the costs of reminders for any overdue liabilities in accordance with the Fee Schedule applicable at the time, default interest at the statutory default interest rate and other costs incurred with debt collection.

The Fee Schedule applicable at the time is published on the Bank’s website.

The user shall be notified of any changes to transaction account fees in the manner described in Chapter 3.18. (Sending notices or informing the user) of these General Terms and Conditions, as a rule one (1) month before the introduction of the change.

The user is obligated to ensure sufficient available account balance at maturity of obligations referred to in this point.

The user undertakes to pay and/or reimburse to the Bank all amounts of duties, taxes, bank fees and other costs paid or incurred by the Bank in relation to the preparing, originating and executing account-related services. provided the duties referred to herein are set forth by applicable laws and regulations.

For international services the Bank carries out for users in Slovenia, fees are charged in domestic currency at the European Central Bank's reference rate applicable as at the date of charge, unless stipulated otherwise.

For other payment transactions which are channelled through other banks or payment agents, the Bank charges additional fees, as charged by those banks or other payment agents for the execution of payment transactions, in accordance with the service fees of all the banks and payment agents involved in the execution of the transaction, with which the user already agrees upon signing the execution of the payment transaction.

As for other payment transactions, the user shall pay the fees for the execution of the payment transaction in accordance with the method of paying fees indicated in the payment order.

When executing domestic and cross-border transactions, each participating bank charges fees to its user of payment services.

3.19.3 Management of average monthly balances

The Bank charges a fee for the management of average monthly balances in the amount and on sums that are over the threshold subject to a fee and on products considered in the calculation of the fee in accordance with the applicable Fee Schedule. Payment of fees is regulated by Subchapter 3.17.6 of these General Terms and Conditions (Transaction account fees).

3.19.4 Exchange rates

In case of currency exchange, the Bank applies exchange rates for corporate customers (hereinafter: exchange rates) in force on the day of the actual execution of the exchange. The exchange rates are published on the Bank's website and at Bank branch offices. The Bank shall publish any changes in the exchange rates on its website or by any other means commonly used in banking. Changes to exchange rates become effective immediately and without any prior notification.

For amounts exceeding EUR 5,000.00 or its foreign currency equivalent, the user can contact the Customer Trading Department (tel. 02 229 2209) and agree on an individual exchange rate in accordance with current market conditions.

The Bank and the user each fulfil their financial obligation under the terms and conditions agreed upon when concluding the transaction (currency pair, amount of purchase or sale of currency, agreed exchange rate) through the appropriate channel for concluding transactions (recorded telephone line, email, trading platform). The user must enter the purchase request in the online bank or arrange the exchange through their account manager in accordance with the Bank's business practice.

For business process and exposure management purposes, currency exchange with settlement dates D+1 and D+2 is treated the same as derivatives. Before concluding such a transaction, the user must contact the Customer Trading Department (tel. 02 229 2209) in order to arrange the contractual relationship and sign the appropriate documentation.

In the event that the Bank or the user is late in fulfilling its obligations, or does not settle the transaction despite the agreement, it is obliged to compensate the counterparty, at its request, for all incurred damage, including damage due to lost profit and compensation due to the cover purchase or sale of an outstanding financial instrument and the like.

The Bank is not liable for any loss that may occur when concluding transactions with the user in the event of *force majeure*, including but not limited to natural disasters (fire, storms, floods), governmental or social measures (war, invasion, civil unrest, labour strikes) and infrastructure failures (traffic, energy), IT failures (including email hacking and cyberattacks), except in the event that the loss was caused by intentional conduct or gross negligence on the part of an employee of the Bank. In this case, the user agrees that the amount of the requested compensation may be at most equal to the amount of the loss on an individual position that would occur due to negligence in the execution of the transaction.

Telephone conversations are recorded and stored in accordance with relevant legislation in order to ensure and verify the correctness of evidence of the transaction. For the purpose of identifying the user, the Bank may

assign a password to the latter, which may be requested before concluding the transaction. The user must handle the password with due care and entrust it exclusively to persons authorised by the company to conclude such transactions.

Payment transactions with a debit card executed in foreign currency are converted into EUR at the exchange rates of the card system (e.g. Visa Europe) applicable at the time of conversion.

3.20 Termination of the Transaction Account Opening and Management Agreement

The Transaction Account Opening and Management Agreement shall be terminated under the conditions specified in this Chapter. The Transaction Account Opening and Management Agreement may be terminated in one of the following ways:

a) With the expiration of time:
The agreement ends with the expiration of time, if it is concluded for a definite period of time.

b) By agreement;
The contracting party and the Bank may mutually agree on the termination of the agreement. The agreement must be concluded in writing.

c) With a notice of termination:
The contracting party may unilaterally terminate the agreement at any time by giving a one-month period of notice, provided this does not breach any other agreements with the Bank and provided they settle all the liabilities arising from the agreement prior to terminating the agreement.

The Bank may terminate an agreement concluded for an indefinite period of time, without specifying the reason, by giving a two-month period of notice. The Bank sends the agreement termination notice to the contractual party by registered mail to the last known address of the contractual party. The notice period is triggered on the day following the posting of the termination notice. In the event of termination of the agreement, the contracting party is obliged to fully settle all obligations under the agreement incurred up to the date of termination of the agreement, including fees charged by the Bank for payment services for a certain period of time, but in a proportional share until the date of termination of the agreement. If such fees are paid in advance, the Bank shall reimburse the contracting party a proportionate share of the fee paid.

The Bank may not charge the contracting party special fees due to the termination of the agreement if the contracting party terminates the agreement concluded for a definite period of more than six (6) months or for an indefinite period, after the expiry of six (6) months from the conclusion of the agreement.

d) Through withdrawal:
The Bank may withdraw from the agreement with immediate effect in the following cases:

- The contracting party has breached the provisions of the Transaction Account Opening and Management Agreement and these General Terms and Conditions;
- The contracting party has overdue liabilities to the Bank;
- The contracting party uses the transaction account for illegal operations or operations that are not in accordance with the indications of the contracting party at the time of establishing the business relationship or do not meet the conditions for maintaining the business relationship defined by the Bank's internal regulations;
- Banking with the contracting party constitutes a violation of the compliance of the Bank's operations, or a violation of the requirements and regulations that the Bank is obliged to comply with, such as, but not limited to, the Prevention of Money Laundering and Terrorist Financing Act, the measures and decisions of the state and judiciary institutions.

The bank sends the notice of withdrawal from the agreement to the user by registered mail. The withdrawal takes effect on the day the registered mail is posted.

Upon termination of the agreement, the Bank terminates the transaction account of the contracting party and, after payment of any overdue liabilities of the contracting party to the Bank in accordance with the provisions of these General Terms and Conditions, transfers any funds remaining in the transaction account to the transaction account indicated by the contracting party. The contracting party authorises the Bank and instructs it to, in the event that the contracting party has funds in a foreign currency on the transaction account, the Bank, upon transferring the funds to another transaction account of the contracting party, converts the funds into the domestic currency at the corporate exchange rate as at the day of the transfer of funds, unless the contracting

party expressly objects to this, namely by means of a written notice sent to the Bank no later than on the day of closing the transaction account of the contracting party, in which it also informs the Bank about the account to which the Bank should transfer the funds. If the contracting party does not notify the Bank of the account, the Bank will transfer the funds to a special temporary account of its choice, where the funds no longer bear interest.

In the event of deletion of the contracting party from the Business Register of Slovenia, the Bank may close the transaction account of the contracting party after the expiry of the notice period specified in the fourth paragraph of this Chapter, of which the Bank shall inform the beneficiary of the funds of the contracting party deleted from the Business Register of Slovenia, in the manner specified in Chapter 3.18. (Sending notices or informing the user) of these General Terms and Conditions. If the Bank does not receive notification of where the funds should be transferred by the closing date of the transaction account of the contracting party deleted from the Business Register of Slovenia, the Bank will transfer the funds to a special temporary account of its choice, where the funds no longer bear interest. In this case, any automatic overdraft on the transaction account is terminated on the day the transaction account is closed.

4. Safe deposit box

The Bank makes the safe deposit box available to the lessee on the basis of the signed safe deposit box lease agreement (hereinafter: the agreement). The agreement can be concluded by any domestic or foreign legal entity or representative office of another country or international organisation which is also a client of the Bank. The agreement is concluded by the lessee's legal representative or a person authorised to represent them. The representative or authorised person must prove their identity based on a valid official identity document and the legal basis for representation with an extract from the registry authority's records, which must not be older than one month, and/or with a written authorisation from the lessee. At the request of the Bank, the lessee is also obliged to submit other information and documents required by the applicable regulations on the prevention of money laundering, tax regulations or other legislation in force in the Republic of Slovenia.

For the duration of the lease, the lessee pays the Bank a rent in the amount agreed in the agreement.

If the lessee wishes to rent several safe deposit boxes, an agreement is concluded for each individual safe.

The lessee cannot transfer their rights under the agreement to another person.

4.1. Duration of the lease

The safe deposit box lease agreement is concluded for the period specified by the lessee and the Bank in the agreement, and after the expiry and new payment of the rent, it is automatically extended for the same period of time as specified in the agreement if the lessee does not inform the Bank at least five (5) days before the expiry of the agreement that they no longer need the safe deposit box.

The Bank informs the lessee about the automatic extension of the lease in the month before the expiry of the lease. If the lessee does not want the agreement to be automatically extended, they must notify the Bank in writing at least five (5) days before the end of the agreement and empty the safe deposit box and return the keys to the safe deposit box.

4.2 Authorisation

The lessee of the safe deposit box may authorise one or more persons to use the safe deposit box. The authorised person may only be an adult, a natural person with legal capacity who must meet the conditions in accordance with the legislation in the field of money laundering prevention and who must be present when the authorisation is issued so that their identity can be verified, and who must sign the acceptance of the authorisation on the Bank's prescribed form.

The authorisation must not contain any restrictions on handling the safe deposit box.

The authorisation ceases to be valid upon written cancellation by the lessee of the safe deposit box, termination of the authorisation by the authorised person, death or termination of the lessee of the safe deposit box or the authorised person, and in the event of termination of the safe deposit box lease agreement. The lessee cancels the authorisation on the prescribed form of the Bank. The cancellation of the authorisation must be notarised, unless it is signed in person in the presence of a bank employee.

If the authorised person cancels the authorisation to use the safe deposit box, they are obliged to return the card for access to the safe deposit box to the Bank, and return to the lessee the key to the safe deposit box which they have in their possession or the magnetic card.

4.3 Safe deposit box keys

Each safe deposit box has two locks. When the agreement is signed and the rent paid, the Bank hands over to the lessee one or two identical keys to the safe deposit box, which may be used by the lessee or their authorised person. The Bank has a bank key that is different from the lessee's key. The Bank may not retain or accept the lessee's key for safekeeping.

The safe deposit box is opened with simultaneous double unlocking, namely, it can be opened by the lessee or an authorised person by opening the first lock with the key received upon the conclusion of the agreement, while the bank employee with the bank key that is different from the lessee's must simultaneously unlock the other lock.

The correct use of the keys when unlocking and locking the safe deposit box, the correct locking of the safe deposit box and the careful protection of the keys are the responsibility of the lessee or authorised person. The Bank is not liable for any damage caused by incorrect use, loss or misappropriation of the lessee's keys. The lessee is also responsible for any incorrect use, loss or misappropriation of the authorised person's keys.

The lessee of the safe deposit box is obliged to carefully store and protect the received keys and must not hand them over to unauthorised persons. Making duplicate keys is not allowed. In case of loss or damage of the keys, the lessee is obliged to notify the Bank of this immediately in writing.

In the presence of the lessee or a notary public, if the properly invited lessee has not responded to the Bank's invitation, the Bank opens the safe deposit box and changes the lock through its authorised contractors. The lessee is obliged to settle all actual costs of opening the safe deposit box, changing the lock and making new keys, other costs specified in the Fee Schedule and any costs of the notary's presence. The lessee is obliged to settle the above-mentioned costs also if the key is lost by their authorised person. At the time of changing the lock, the lessee is obliged to remove the contents from the safe deposit box.
After the termination of the agreement, the lessee is obliged to empty the safe deposit box and return to the Bank all the keys received when renting the safe. The lessee and a bank employee check together that the safe deposit box is empty.

If the lessee does not empty the safe deposit box and return the keys after the expiry of the agreement, the Bank shall charge them a fine in the amount of the full annual rent, regardless of the number of days of delay, in accordance with the Fee Schedule.

4.4 Safe deposit access card

The Bank issues to the lessee and their possible authorised persons a card for access to the safe deposit box, with which, together with a valid official personal identification document with a photo, they prove that they are the lessee of the safe deposit box or that they are authorised to use the safe deposit box.

In case of loss the card, the lessee is obliged to notify the Bank of this immediately in writing. The Bank shall issue a new card to the lessee or their authorise persons, which will show that it is a duplicate. The cost of making a new card shall be borne by the lessee of the safe deposit box.

Upon expiration or termination of the safe deposit box lease agreement, the lessee is obliged to return all issued safe deposit box access cards to the Bank.

4.5 Safe deposit access magnetic card

In branches where magnetic cards are used for access to safe deposit boxes, the Bank issues a magnetic card for access to the safe deposit box to each of the lessee and their possible authorised persons.

The Bank shall grant access to the safe deposit box to the lessee or any their authorised person by the lessee or their authorised persons inserting their magnetic card into the reader and entering their personal identification number (PIN). The personal identification number (PIN) is determined by the lessee or the authorised persons themselves. The PIN number consists of four digits and must not contain recorded data (e.g. the user's date of birth, ID card number, etc.) or logical sequences (e.g. 1234, 1111, etc.).

It is the lessee's duty to use the magnetic card and PIN number correctly and to protect them carefully. The Bank is not liable for any damage caused by incorrect use, loss or misappropriation of the lessee's magnetic card.
In case of loss of the coded magnetic card for access to the safe deposit box, the lessee is obliged to immediately notify the Bank of this in writing. The same applies if an unauthorised person knows the personal identification number (PIN) or if there is only suspicion about it. The Bank shall cancel the lost magnetic card and issue a new one to the lessee or their authorised person after receiving a written notification. The lessee shall pay for the issuance of the new magnetic card in accordance with the Fee Schedule.

After the termination of the safe deposit box lease agreement, the lessee is obliged to empty the safe deposit box and return the magnetic cards of the lessee and any authorised persons. The lessee and a bank employee check together that the safe deposit box is empty.
If the lessee does not return the magnetic card after the expiry of the agreement, the Bank shall charge them a fine in the amount of the full annual rent and the relevant Bank’s costs in accordance with the Fee Schedule.

4.6 Access to the safe deposit box

Only the lessee or their authorised person shall have access to the safe deposit box during the business hours of the Bank's branch where the safe deposit boxes are located. The business hours of the area with the safe deposit boxes may differ from the business hours of the Bank's branch where the safe deposit boxes are located. The Bank may change the business hours if necessary.

Before entering the area with the safe deposit boxes, the lessee or authorised person must show the bank employee the safe deposit access card and a valid official identification document with a photo and sign the record card of the safe deposit box.
The lessee is obliged to respect the security system in the area where the safe deposit boxes are located. Only two people can access the same safe deposit box at the same time.

Access to the safe deposit box is only possible in the presence of a bank employee.

In case of liquidation of the lessee, the Bank shall deny the authorised person access to the safe deposit box.

4.7 Storage of items in safe deposit boxes

Safe deposit boxes may be used to store objects and documents, except for objects and substances that are perishable and subject to disintegration, or objects whose possession and traffic with them are prohibited by law and with which it is possible to cause a general danger which is considered a criminal act in accordance with Article 314 of the Criminal Code, namely objects or substances that can be flammable, explosive, radioactive, etc., as well as drugs and weapons. It is not allowed to keep cash in the safe deposit box.

In suspicious cases, the bank employee has the right to check the content that the lessee wishes to store in the safe deposit box in the presence of the lessee, but only to determine its suitability for safekeeping, and not with regard to its value.

The lessee shall be liable for any damages due to the damage caused to the Bank or to other safe deposit box lessees by the items referred to in the first paragraph.

If the lessee does not comply with the obligations from the first paragraph of this Article, the Bank may terminate the agreement.

4.8 Reminder procedure and pre-emptive right of the Bank

After the end of the lease period or after the termination of the agreement, the lessee is obliged to empty the safe deposit box, return all keys to the safe deposit box, or magnetic cards, return all safe deposit access cards and settle any outstanding obligations.

The Bank confirms the receipt of the keys/magnetic cards with a written confirmation of the receipt of the keys/magnetic cards in two (2) copies, one of which is given to the lessee and the other to the Bank.

If the lessee does not act in accordance with the first paragraph of this Subchapter, the Bank shall send them a written reminder to do so within eight (8) days. If the lessee does not fulfil their obligations referred to in the first paragraph within the additional period, the Bank shall start collection procedures and/or, within two (2) months

after the termination of the agreement, the safe deposit box will be forcibly opened in the presence of a notary public who will make a list of the contents of the safe deposit box. The list of the contents shall be sent to the lessee of the safe deposit box in the contractually agreed manner.

The costs of forcible opening of the safe deposit box and the notary's services shall be reimbursed by the lessee to the Bank immediately upon the Bank's first written request, and the Bank shall also be entitled to recover such costs in accordance with the provision of the next paragraph.

The Bank shall have a pre-emptive right on any items found in the safe deposit box, to repay any payment obligations of the lessee to the Bank, any damage and expenses incurred, by repaying out of the money found in the safe deposit box or out of the proceeds obtained from the sale of the items found in the safe deposit box. The remainder of the items found in the safe deposit box which are not used by the Bank to satisfy its claims against the lessee shall be kept by the Bank at the lessee's expense. The storage period for items found in the safe deposit box is five (5) years from the date the safe deposit box was opened. After the expiry of this period, the items will be destroyed by commission or sold at an auction.

The lessee expressly and irrevocably authorises the Bank and gives it a standing order to use and debit all funds that the lessee has or will have in the transaction account with the Bank for the payment of overdue obligations under the agreement, without a special order.

4.9 Items found

For items found in the premises where the safe deposit boxes are located, the Bank shall prepare a record and act in accordance with the applicable regulations governing the handling of items found.

4.10 Relocation of safe deposit boxes

If a branch is renovated or refurbished, or when safe deposit boxes are moved to other locations due to the closure of a bank branch, the Bank shall inform the lessees of the safe deposit boxes of its intention in writing, specifying the possible new location of the safe deposit boxes and the possibility of providing a replacement safe deposit box for the duration of the renovation or refurbishment of the branch, and ask them to empty the safe deposit boxes. The lessees shall have 30 days after receiving the notice available to empty their safe deposit boxes.

The Bank shall provide a replacement safe deposit box to the lessee during the renovation or refurbishment of the branch, subject to availability and the lessee's consent. If it is not possible to provide a replacement safe deposit box or if the lessee does not agree with it, the Bank shall refund a proportional part of the rent for the time when they cannot use the safe deposit box. After the completion of the renovation or refurbishment, the lessee will again be able to use the safe deposit box in accordance with the safe deposit box lease agreement and these General Terms and Conditions.

If safe deposit boxes are moved to a new location due to the closure of a branch, the Bank shall provide the lessee with a safe deposit box at another location and the lease shall continue under the same conditions at such other location. If the lessee does not agree with the relocation and notifies the Bank thereof in writing within (30) thirty days of the receipt of the notice, the lease agreement shall cease to be valid, regardless of the period for which it was concluded, within eight (8) days of the Bank's receipt of the lessee's statement that they disagree with the new location. In this case, the lessee is obliged to act in the manner agreed upon for the termination of the safe deposit box lease agreement (empty the safe deposit box, return the keys or magnetic cards, return the access cards and settle any outstanding obligations) and the Bank shall return a proportional part of the rent for the period from the termination of the agreement to the expiration of the contractually agreed lease period.

If the lessee fails to respond in time to the Bank's notice referred to in the first paragraph of this Chapter, it shall be deemed that the lessee agrees with the safe deposit box relocation and the Bank shall not be liable for any damage to the contents of the safe deposit box.

4.11 Responsibility of the Bank

The Bank shall ensure the safety of the safe deposit boxes with due professional care. The Bank shall ensure that appropriate and prescribed security measures are implemented in the protection of the premises in which the safe deposit boxes are located.

The Bank shall be liable to the lessee of the safe deposit box for any property damage only if caused and proved to have been caused by the Bank's failure to take precautions or otherwise to act in a diligent manner. Since the Bank is not aware of the contents of the safe deposit boxes, only the lessee who shows the contents of the safe

deposit box on the day of the loss event has the right to compensation for the items for which compensation is requested. The lessee must also prove the value and ownership of the items for which they request compensation.

The lessee is not entitled to compensation for damage if they keeps items contrary to the provisions of these General Terms and Conditions.

The Bank shall not be liable for damage due to events beyond its control and in case of *force majeure*. The Bank is also not responsible for the contents of the safe deposit box after the termination of the lease agreement, or after the notice of termination of the agreement has been sent and the lessee has not emptied the safe deposit box by the end of the notice period.

4.12 Termination of the agreement

The Bank may withdraw from the agreement in writing before the expiry of the lease period and with immediate effect if:

- The lessee does not pay the rent or other costs;
- The safe deposit box is used to keep items which may not be kept in it in accordance with these General Terms and Conditions;
- The lessee does not allow the bank employee to check the contents of the safe deposit box in accordance with these General Terms and Conditions;
- The lessee and/or authorised person violate the provisions of the safe deposit box lease agreement or the provisions of these General Terms and Conditions;
- The lessee is no longer a client of the Bank (no longer has an open business transaction account).

The Bank may terminate the agreement in writing before the end of the lease period, with thirty (30) days' notice, upon closing the Bank's branch and in case of non-fulfilment of the conditions for establishing or maintaining a business relationship, in accordance with the Bank's business policy.

If the Bank does not want to extend the agreement by the same lease period, it must notify the lessee thereof at least thirty (30) days before the expiry of the lease period.

The Bank shall send the notice of termination of or withdrawal from the agreement, or the notice that it does not want to extend the agreement, to the lessee in the contractually agreed manner. The Bank shall send the notice of termination or withdrawal on paper to the lessee's last known address. The notice period shall begin the day after the notice of termination is sent by mail, or after the receipt of the notice when the Bank terminates the agreement via a permanent data carrier.

The lessee may terminate the agreement in writing before the expiry of the lease period and with immediate effect if all of the following conditions are cumulatively met:

- The rent and all obligations under the safe deposit box lease agreement have been paid in full at the time of termination;
- the safe deposit box has been completely emptied;
- the lessee (including any authorised person) has returned all keys to the safe deposit box or magnetic cards for access to the safe deposit box received at the time of the lease;
- the lessee has returned the card for accessing the safe (including the card for any authorised person).

In the case referred to in the first and fifth paragraphs of this Chapter, the lessee is not entitled to a refund of the rent already paid. In the case referred to in the second paragraph of this Chapter, the lessee is entitled to a refund of a proportional part of the rent already paid.

5. Post office operations

The following payment transactions are possible at the post office via the user's transaction account:

- Cash deposits to and withdrawals from the transaction account in domestic currency;
- Payment of payment orders.

In order to make payments, the authorised person must have an appropriate authorisation, a valid debit card and/or a valid personal identity document.

6. Common provisions

6.1. Protection of personal and confidential data

Information and data relating to the performance of payment and other services shall be treated as business secrets of the Bank. The Bank shall only disclose these data to the user of payment and other services and to the authorities competent in accordance with the law upon their written request.

The Bank, as the controller of the personal data collection, manages, maintains and controls the collection of personal data and data about the user and their authorised persons pursuant to the Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR, EU 2016/679) and in accordance with the act on personal data protection applicable at the time, as detailed in the General Information on Personal Data Protection in OTP banka, available on the Bank's website and at its branches.

The Bank may collect, process and exchange the following confidential data, including the user's personal data, for the purpose of preventing, investigating or detecting fraud or scams in connection with payment and other services:

– information about users of payment and other services, their legal representatives, authorised persons and third parties who are involved in fraud or scam or an attempt thereof, or have suffered or could suffer damage as a result of such an event or attempt thereof: name and surname or company name, permanent and/or temporary place of residence or registered office, citizen ID number, tax number, data on payment accounts, card data of these persons and data on the balance and transactions on these accounts, the method of authentication of the payer used and identification, authentication and communication data (telephone number, email address, IP address, audit trails, correspondence with the client and other data of this type necessary for the efficient handling of the case), and the date and description of the events related to the fraud or scam or the attempt thereof, and the amount of the payment transaction in question.
–
On the basis of the Prevention of Money Laundering and Terrorist Financing Act and the Customer Acceptance Policy applicable at the time, in order to establish a business relationship, the Bank must carry out identification establishment and verification procedures; consequently, it requests that the user, authorised person and legal representative provide personal data specified by law and submit a personal identity document to be copied. Providing the required data is a legal and contractual obligation, which means that the Bank shall not enter into a business relationship or terminate it if it does not obtain all the required data.

In accordance with the above-mentioned legal bases and for the purpose of preventing, investigating or detecting fraud and scams in connection with payment services or money laundering, the Bank may request from the user, before entering into and continuing the existing business relationship, additional information and evidence, including but not limited to the following:

- Tax number, company registration number, citizen ID number;
- Activity of the legal entity:
- Information on the political exposure of the legal representative, authorised person or beneficial owner;
- Amount of equity stake or other type of control of the beneficial owner;
- Purpose and envisaged nature of the business relationship;
- Date, time, purpose, currency and method of execution of the transaction;
- Data on the intended recipient of the transaction;
- Destination country of the transaction;
- other information and evidence that the Bank may request in order to avoid violation of legal provisions and internal regulations of the Bank.

The user expressly authorises the Bank to establish, process, store or forward personal and other data related to the provision of payment and other services in accordance with these General Terms and Conditions using automatic processing means or traditional means.

The Bank may collect, process and exchange confidential data, including personal data about the user, also for the purpose of providing the service of ordering payments and the service of providing information about accounts, but only to the extent that still enables the performance of the aforementioned services, and in cases of disclosure of personal and confidential data of the user, if the payment transaction was carried out based on the erroneous use of the identification mark.

The user expressly allows the Bank to carry out an inquiry and obtain information about their personal and other data, including in particular about employment, movable and immovable property, claims, stakes, shares and other securities, numbers of accounts with banks and payment institutions, and other user's property, place of residence, tax number and other data from other database operators, if the Bank does not have them or, despite its request, the user has not personally provided them to the Bank and these data are necessary to achieve the purpose of these General Terms and Conditions and the agreement concluded on the basis of these General Terms and Conditions.
The user agrees with the processing of personal data and also allows the processing of personal data that they have provided to the Bank or that the Bank has at its disposal, for the purposes of fulfilling contractual obligations as well as fulfilling the Bank's relevant legal and regulatory obligations and obligations assumed by the Republic of Slovenia and in accordance with international legal acts and acts of the European Union adopted by the Republic of Slovenia, and all binding national and international acts and rules applying or relating to the prevention of money laundering and terrorist financing, and the implementation of the international agreement between the Republic of Slovenia and the USA regarding the Foreign Account Tax Compliance Act (FATCA), OECD automatic financial account data exchange (Common Reporting Standard – CRS) and the Tax Procedure Act (ZDavP).

6.2. Sanctions

“Sanction” means any act, regulation, order, restriction or other requirement relating to economic, financial or trade sanctions adopted, ordered, imposed or publicly announced by a government, any official institution, body or agency of the:

- United Nations Organisation; European Union;
- United States of America;
- United Kingdom of Great Britain and Northern Ireland (HMT Treasury and Bank of England).

“Country under sanctions” means any country or other territory subject to state or territory sanctions, or any country or other territory whose government is subject to state or territory sanctions.

“Person under sanctions” means a person subject to sanctions.

The Bank shall not enter into business relationships or transactions with persons subject to sanctions. In addition, the Bank shall not carry out payment transactions to legal or natural persons directly or indirectly connected to Syria, Sudan, North Korea, Cuba, Iran or the area of Crimea, Donbass (Donetsk and Luhansk regions), or Kherson and Zaporozhye regions in Ukraine in accordance with the Customer Acceptance Policy and the Money Laundering and Terrorist Financing Prevention Policy, published on the website https://www.otpbanka.si/preprecevanje-pranja-denarja-cap-politika.

6.3 Amicable settlement of disputes

The user and Bank shall settle any disputes, disagreements or complaints relating to the performance of services in accordance with these General Terms and Conditions in an amicable manner.

The user may file a complaint regarding a service rendered by the Bank in person, by mail to the address of the Bank or by email to info@otpbanka.si. The user can also submit a complaint regarding the use or operation of the eBank@Net com electronic bank, the Bank@Net com online bank or the mBank@Net com mobile bank to the Bank by means of a notification provided for in the eBank@Net com electronic bank, the Bank@Net com online bank or the mBank@Net com mobile bank, by email at bankanet@otpbanka.si or by phone at 080 17 70 or at other phone number that the Bank communicates to the user.

The Bank decides on the complaint after collecting all the documentation within fifteen (15) business days at the latest. The decision on the complaint shall be sent in writing to the user's address.

Where, in exceptional cases, for reasons beyond its control, the Bank cannot reply within fifteen (15) business days, the Bank shall provide the user with an interim reply, in which it will clearly state the reasons for the delay and set a deadline by which the user will receive the final answer. The deadline shall not exceed thirty-five (35) business days.

Any disputes arising out of these General Terms and Conditions the user and the Bank cannot resolve in an amicable manner shall be settled in the court of competent local jurisdiction according to the registered office of

the Bank. Notwithstanding the above, the Bank may, at its discretion, initiate appropriate legal proceedings before any other locally competent court.

The Bank and the user agree that they will mutually recognise in court the validity of electronic messages provided in the software package of the eBank@Net com electronic bank, the Bank@Net com online bank and the mBank@Net com mobile bank.

Any complaints arising from the content of e-documents shall be resolved by the recipient of the e-document directly with the issuer of the e-document. The Bank shall not handle such complaints. If the complaint is of a technical nature, it shall be resolved by the bank receiving the e-document.

The user of payment services can file a complaint with the Bank of Slovenia regarding alleged violations of the Payment Services, Electronic Money Issuing Services and Payment Systems Act (ZPlaSSIED).

6.4 Deposit guarantee

A credit balance on a transaction account, savings deposits and other deposits are eligible for the guarantee under the Deposit Guarantee Scheme Act (hereinafter also ZSJV).

If the Bank becomes insolvent, the depositors are paid from the deposit guarantee scheme.

The maximum deposit guarantee is EUR 100,000 per investor in a bank, meaning that all eligible deposits of the depositor with the bank are added up. In some cases laid down by the ZSJV, deposits are protected even above this limit.

Information for depositor about the deposit guarantee scheme is published on the Bank's website Information for depositors concerning the Deposit Guarantee Scheme.

6.5 Final provisions

The following documents form an integral part of these General Terms and Conditions:
- Domestic, Cross-Border, and Other Payment Transactions Schedule;
- Fee Schedule for transactions with legal entities, self-employed persons, sole proprietors and associations;
- Decisions on interest rates;
- General information for depositors concerning the Deposit Guarantee Scheme
- eBank@Net com, Bank@Net com and mBank@Net com Application;
- Designation of authorised person or revocation of authorisation for eBank@Net com, Bank@Net com and mBank@Net com;
- Application form for performing services through Poslovni Bank@Net;
- Authorisation for performing services through Poslovni Bank@Net.

The Bank may change the general terms and conditions or adopt new general terms and conditions to replace these General Terms and Conditions, of which it shall inform the user that is also a user of the electronic bank through Poslovni Bank@Net, the eBank@Net com electronic bank, the Bank@Net com online bank or via the mBank@Net com mobile bank, or to the last notified email address, and otherwise by mail, as a rule one (1) month before the proposed date of commencement of application of the amended and/or supplemented or new General Terms and Conditions. The amended and/or supplemented or new General Terms and Conditions shall be published on the Bank's website.

If the user does not agree with the changes to the General Terms and Conditions, they may terminate the agreement concluded on the basis of these General Terms and Conditions without a notice period and payment of fee up to the day before the proposed date for the changes to come into effect. If the user refuses the change to the General Terms and Conditions, but does not terminate the agreement, the Bank is considered to have terminated the agreement with a two-month notice period starting from the date of sending the notification of the change. If the Bank does not receive the user's statement that they are terminating the agreement concluded on the basis of these General Terms and Conditions, or the user does not notify it within this period that they do not agree with the proposed changes, the user shall be deemed to have agreed to the changes.

The General Terms and Conditions applicable at the time are published on the Bank's website and available in all Bank's branches.

These General Terms and Conditions form an integral part of the agreement. By signing the agreement, the user confirms that they were aware of them before concluding the agreement and that they fully agree with them.

In the event of a discrepancy between these General Terms and Conditions and the agreement, the provisions of these General Terms and Conditions shall apply.

These General Terms and Conditions shall also apply to existing contractual relationships in connection with leasing a safe deposit box, opening and managing a transaction account, operations with Visa business payment cards, approved extraordinary overdrafts on transaction accounts, as well as existing contractual relationships for standing orders and SEPA direct debits.

For existing contractual relationships in connection with the approved extraordinary overdraft on transaction account, based on the request for overdraft, the notice of overdraft approval and the general terms and conditions for authorised overdrafts on the transaction account, which together constitute the agreement, the general terms and conditions for authorised overdrafts on the transaction account shall continue to apply until the expiration of this agreement.

Provisions of the agreement with which the Bank and the user regulated the contractual relations regarding the opening of the transaction account and the provision of payment services until the entry into force of these General Terms and Conditions and which are in conflict with the provisions of the ZPlaSSIED shall be considered to have been replaced by the provisions of the ZPlaSSIED.

If the user becomes aware of a breach committed in carrying out services under these General Terms and Conditions, and such a breach constitutes an infringement under the ZPlaSSIED, they shall have the right to file a written motion to open infringement proceedings. The motion shall be filed with the Bank of Slovenia, which is the authority competent to decide in matters concerning infringements.

By these General Terms and Conditions, the Bank and the user agree to exclude or restrict the application of the following provisions of the ZPlaSSIED: Articles 87 to 110, 122 (except paragraph 3 of this Acticle), 123, 137, 140, 142, from 146 to 148 and 150 of the ZPlaSSIED, and Article 4, fifth and sixth paragraphs, of Regulation (EU) 2021/1230 of the European Parliament and of the Council of 14 July 2021 on cross-border payments in the Union (hereinafter: Regulation 2021/1230), which shall be replaced by the relevant provisions of these General Terms and Conditions.

With the issuance of these General Terms and Conditions, the existing General Terms and Conditions for the provision of payment services for legal entities, self-employed professionals, sole proprietors and associations, the General Terms and Conditions for transactions with Mastercard and Visa business payment cards, and the General Terms and Conditions for transactions with prepaid Visa cards for legal entities, sole proprietors and self-employed professionals, the General Terms and Conditions for the use of the eBank@Net com electronic bank, the Bank@Net com online bank and the mBank@Net com mobile bank, and the General Terms and Conditions for the use of Poslovni Bank@Net shall cease to apply.

With the issuance of these General Terms and Conditions, the General Terms and Conditions for maintaining a transaction account and providing payment services for legal entities, owners of private businesses and civil law entities, the General Terms and Conditions for business with Visa business debit card and Visa business credit card, the General Terms and Conditions for using the security SMS service and Info SMS, the General Terms and Conditions for the use of digital banking for legal entities, owners of private businesses and civil law entities, and the General Terms and Conditions for leasing a safe issued by SKB banka d.d. shall also cease to apply.

The user has the right to request a copy of the General Terms and Conditions on paper or another permanent data carrier at any time.

The Slovenian language shall be used for contractual relations and communication between the Bank and the user, unless the Bank and the user agree otherwise.

The law of the Republic of Slovenia shall apply to the provision of services in accordance with these General Terms and Conditions and their interpretation.

These General Terms and Conditions shall enter into application on 1 September 2024.