GENERAL TERMS AND CONDITIONS OF CONSUMER BANKING

Obr. 3918 RA-146/21

TABLE OF CONTENTS

1 INTRODUCTORY PROVISIONS

These General Terms and Conditions of Consumer Banking ("T&Cs") govern the rights and obligations of the Bank and the user (consumer) concerning:

- Use of payment services via transaction accounts held with the Bank;
- Payment instruments;
- Use of the Savings Account;
- Use of the Triple Plus savings account;
- Use of ZA-TO! savings product;
- Use of Individual Retirement Account;
- Deposit products;
- Safety deposit box hire.

These T&Cs are issued by:
OTP banka d. d. ("OTP banka d. d."), Slovenska cesta 58, 1000 Ljubljana, Slovenija, SWIFT code KBMASI2X, registered with the District Court of Ljubljana, registration number: 5860580000, VAT ID number: SI94314527. OTP banka d. d. is on the list of banks and savings banks authorized by the Bank of Slovenia to provide payment services, as published on the Bank of Slovenia website. The competent supervisory authority of the issuer of these T&Cs is the Bank of Slovenia.

2 DEFINITION OF TERMS

Terms used in these T&Cs shall have the following meaning:

AUTHENTICATION: procedure that allows the payment service provider to verify the identity of a payment service user or the eligibility to use of a specific payment instrument, including the use of the user's personalised security credentials.
AUTHORIZATION: a process by which the provider of goods and services or an ATM obtains confirmation from the Bank allowing it to execute the transaction.
Bank@Net: online banking of OTP banka d. d.
BANK: OTP banka d. d.
ATM: an automated electronic device by means of which the payment card holder can withdraw cash from their transaction account and execute other cash transactions.
CONTACTLESS TRANSACTION: a quick, secure and simple transaction; it is made by tapping the card or mobile device against the designated area of the POS terminal. Transactions up to a certain amount do not require of the user to enter the PIN. This amount varies from country to country; the amount valid for Slovenia is published on the Bank's website.
CONSUMER BANKING FEE LIST: applicable fee list for banking services of OTP banka d.d. ("Fee List").
CLICK TO PAY: simple and secure way to pay without having to enter card details manually.
CVC/CVV: a three-digit verification number printed on the back of the card next to the signature strip.
CROSS-BORDER PAYMENT TRANSACTION: 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: reference period used by the Bank for accounting interest on funds debited or credited to the payment account.
DCC: not a service of OTP banka, but a service of the merchant or ATM that allows the execution of a card-based payment transaction with immediate conversion into EUR at the rate set for the exchange by service provider DCC.
VISA DEBIT CARD: a card with immediate debit/authorization of balance on the transaction account.
BUSINESS DAY: any day on which the payer's payment service provider or the payee's payment service provider involved in the execution of a payment transaction is open for business and facilitates the execution of payment transactions for its user.
DEPOSITOR: a natural person who enters into a Term Deposit Agreement with the Bank.
DEPOSIT: cash balances deposited by the depositor with the Bank that the Bank has the right to use, however, is required to return them under terms stipulated by the agreement.
DAILY DIGITAL BANKING SPENDING LIMIT: maximum amount of all payments made from the account in a single day, as shown in the digital bank. The daily account spending limit (either on the primary account or an account the user is authorized to use) does not include money transfers between primary accounts or accounts the user is authorized to use, to and from savings products, and to and from pre-paid cards.
DIGITAL BANK: the umbrella term for Bank@Net online bank and mBank@Net mobile bank.
DIGITAL CARD: card in digital format stored on the cardholder's mobile device that is used to make contactless payments via the cardholder's mobile device.
DOMESTIC PAYMENT TRANSACTION: 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: 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 a Member State's currency.
MEMBER STATE: a European Union member state or a state signatory of the European Economic Area (EEA) Agreement.

EMV: technical standard for card payments that ensures secure transfer of card data.
ONE-TIME MOBILE WALLET PASSWORD: randomly generated sequence of characters that changes and is valid only once. It also the password that the user received via SMS to their mobile phone number and is used to register for the mobile wallet.
UNIQUE IDENTIFIER: a combination of letters, numbers or characters assigned by the payment service provider to the user and used in A payment transaction for unambiguous identification of the user and their payment account.
E-NOTIFICATION: notification in electronic format. Also available in the banking portal eNotifications.
E-INVOICE: invoice issued in standard electronic format and in accordance with regulations governing this line. An E-invoice is an equivalent replacement for a paper invoice that the invoice issuer distributes to the invoice recipient for a service rendered, goods delivered, etc. It can also be sent to the digital bank.
QUICK LOGIN (mPassword): the user can use the mPassword or biometrics to log into mBank@Net via the app.
FLIK PHONEBOOK: solution used to obtain data about the transaction account of the payee or payer to execute a Flik instant payment order or send a request for a Flik instant payment based on contact data (pseudonym/alias).
SAVINGS ACCOUNT HOLDER: natural person who enters into a Savings Account Agreement with the Bank.
CARD HOLDER: consumer to whom the Bank issued a payment cards in accordance with these T&Cs.
PREPAID ACCOUNT HOLDER: consumer who applied with the Bank for a prepaid card and for whom the Bank opened a prepaid account.
ACCOUNT HOLDER: natural person for whom the Bank opens an account by their request and subject to these T&Cs to execute payment transactions and for other purposes associated with banking services.
SAFETY DEPOSIT BOX ACCESS CARD: card that the Bank provides to the safety deposit box renter and any authorized users of theirs.
CHARGE CARD: a payment card where the card holder repays the total card debt once per month on the chosen day by way of a direct debit to the transaction account.
CARD ACCOUNT: the account to which all card-based payments (primary and any authorized cards) are debited.
CONTACT DATA (pseudonym/alias): mobile phone number of Slovenian mobile network operator and/or user's email address that the user securely communicated to the Bank and later activated it in the Flik mobile app to use the Flik Phonebook or liked the email address with their personal account with the Bank in the mobile wallet app.
CREDIT TRANSFER: 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: the aggregate of credit balance in the transaction account (in domestic and foreign currencies) and authorised overdraft facilities available on the transaction account.
mBank@Net: the Bank's mobile banking.
mPASSWORD, MOBILE PASSWORD: personal password that the user uses in the mobile app for quick login to mBank@Net. It is a combination of at least six (6) characters that the user can change as frequently as they please.
MOBILE DEVICE: mobile phone running Android or iOS operating system that supports the installation and use of the mobile wallet and mBank@Net app or tablet, other device, or wearable (e.g. watch) that supports the installation of the mobile wallet and exchange of data between the mobile device and POS terminal without direct contact (NFC technology) or with a camera used to read the QR code.
MOBILE WALLET: app available from Google Play and the App Store that the user can install on their mobile device and add to it their payment cards in digital format to pay for goods and services or use it for Flik payments.
MOBILE TOKEN: system used to generate passwords via the mBank@Net mobile bank.
MOČNA AVTENTIKACIJA STRANKE: 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 designed so as to protect the confidentiality of data being verified.
INBOX: mailbox in the digital bank used to receive e-invoices, messages about market campaigns and new products, and other messages.
RENTER: domestic or foreign natural person who enters into a Safe Deposit Box Rental Agreement.
RENTAL FEE: 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.
NFC (ang. near field communication): technology that facilitates data exchange between the mobile device and the POS terminal without direct contact.
ACCOUNT ACTIVITY NOTIFICATIONS: SMS and/or email distribution service with information on transaction account balance, incoming/outgoing payments, end of term of deposit, end of authorized overdraft, successfully processed and/or rejected payments, or incoming SEPA Direct Debits.
PERSONAL SECURITY CREDENTIALS: personalised features provided by the payment service provider to a payment service user for the purposes of authentication.
PERSONAL PASSWORD or PASWORD: combination of a sequence of six (6) numerical characters chosen by the user themselves.
PRIMARY CARD: card issued to card account holder.
PAN: sixteen-digit card number.
BUNDLED OFFER: set of banking services in the scope as outlined by these General Terms & Conditions that the bundle holder uses for a single monthly fee.
PIN (Personal Identification Number): personal identification number consisting of four or six characters in sequence.
PAYMENT CARD: payment instrument issued by the Bank to the user that can be used to make transactions at ATMs, points of sale and online points of sale, and to pay with the mobile wallet.

PAYMENT SERVICES: activities that facilitate the deposit of cash to a transaction account and withdrawal of cash from a transaction account and all the activities necessary to manage this account, execute payment transactions debited and credited to this account (via direct debits, payment cards, or similar devices or credit transfers), execute payment transactions where cash balances are provided by approving a loan to a user (via direct debits, payment cards, or similar devices or credit transfers), issue payment instruments and/or acquire payment transactions, execute money transfers, payment initiation services, and provide account information services.
PAYMENT TRANSACTION: 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 a payment transaction through the payment service provider is independent of the basic obligations between the payer and payee.
PAYMENT INSTRUMENT: any device or set of procedures (or both) agreed upon between the user and their payment service provider that is linked to this user only for the purpose of initiating a payment order.
PAYMENT ORDER: an instruction by which the payer or the payee instructs their payment service provider to execute a payment transaction.
PAYMENT ACCOUNT: account opened by the payment service provider on behalf of one or more users that is used to execute payment transactions.
PAYMENT: request to execute a payment transaction.
PENDING PAYMENT: payment that will be executed in the future, not on the day it was confirmed, by request of the user. Once the payment has been confirmed using personalized security credentials, it is given the status of ending payment during the term ending with the selected payment date.
PAYER: natural or legal person who initiates a payment transaction by issuing a payment order or approving the execution of a payment order issued by the payee.
CONSUMER PAYMENT SERVICES AGREEMENT: agreement based on which the consumer has opened a transaction account and based on which they use services of the Bank (e.g. Business Cooperation Agreement).
E-NOTIFICATIONS PORTAL: secure electronic channel used to distribute e-notifications.
CONSUMER: natural person who enters into agreements and uses banking services outside of their professional or gainful activity.
AUTHORIZED USER: natural person of legal age and full capacity to contract, whose entitlement to representation is based on authorization.
AUTHORIZED USER CARD: a card issued to the authorized user of the card account held by the account holder by request of the card account holder or by request of the card holder, subject to consent by the card account holder.
POS TERMINAL: 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.
PREPAID CARD: a debit card that a card holder can use to make payments within the available prepaid account balance.
PREPAID ACCOUNT: an account linked to the prepaid card and to which the card payments are credited or debited.
PAYEE: any natural or legal person that is the intended recipient of funds subject to the payment transaction.
TRANSFER BETWEEN ACCOUNTS: transfer of balances between transaction accounts (own and authorized).
VERIFICATION OF PAYEE (VOP): verification of match between payee's name and IBAN for all credit transfers (domestic and cross-border).
DEFAULT PAYMENT INSTRUMENT: payment instrument (payment card) that the user selects in the mobile wallet as the primary instrument to execute a payment transaction (applies only to mobile devices running Android operating system).
PROCESNI CENTER: 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: the provider of goods and services that accepts payment cards as A payment method. A point of sale is equipped with a label of the payment card brands it accepts.
AVAILABLE TRANSACTION ACCOUNT BALANCE: balance of the transaction account in the currency of payment, increased by any authorized overdraft in domestic currency and reduced by other sums owed arising from transaction account activity (e.g. authorization of funds, pending payment orders on a particular date, transactions not yet booked).
REGULAR AUTHORIZED OVERDRAFT: predetermined amount of authorized negative balance on the personal account that the Bank can approved on the account as an authorized overdrawn balance.
€STR (Euro short-term rate) REFERENCE RATE, whose daily values are posted on the Euro short-term rate (€STR) website (europa.eu).
REFERENCE EXCHANGE RATE: daily exchange rate by which the Bank of Slovenia reports currency exchange rates.
SAFE DEPOSIT BOX: a special metal drawer built into a secure and protected area of the Bank used to store belongings.
SEPA DIRECT DEBIT (abbrev. Sepa DB): a payment service where the payee makes an order to debit the payer's payment account based on the payer's consent.
REMOTE CONTRACTING: an agreement that the Bank and the user enter into remotely without the parties being present in person at the same time until and including the moment when the agreement takes effect.
DECISION ON INTEREST RATES: applicable Decision on interest rates of OTP banka.
CUSTODIAN: natural or legal person whose right to represent is based on a decision of the competent authority.
SMS TOKEN: one-time password that the card holder or digital bank user receives in an SMS sent to their mobile phone and is used exclusively to log into the digital bank and confirm a payment or request. The card holder is obligated to verify the contents of the SMS (e.g. amount and currency of payment shown in the SMS they received) before confirming the payment or request.
CONSENT TO EXECUTE PAYMENT TRANSACTION: the act of the user providing the Bank or payment initiation service provider with a paper-based or electronic payment order or the act of the user providing authorization to execute a payment transaction if the transaction is initiated by the payee or payment initiation service provider.
BANK'S WEBSITE/URL: otpbanka.si.
PAYMENT INITIATION SERVICE: service to initiate a payment order by request of the payment service user concerning a payment account held with a different payment service provider.

ACCOUNT INFORMATION SERVICE: online service providing consolidated information about one or more payment accounts held by the payment service user with a different payment service provider or one or more payment service providers.
INSTANT PAYMENT: credit transfer available 24/7 that is executed in a few seconds.
STANDING ORDER: an instruction by which the payer instructs their payment service provider to execute credit transfers regularly or at previously determined dates.
DURABLE MEDIUM: any instrument allowing the user to store data or information addressed to them personally in a permanent manner, with permanent access, and the option to reproduce them. These media include in particular paper, USB drive, CD-ROM, DVD, memory drives or computer hard drives and email. A website is not regarded as a durable medium.
TRANSACTION ACCOUNT (TA): a payment account opened by a bank registered in the Republic of Slovenia 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: any state other than an EU Member State or a signatory state to the European Economic Area (EEA) Agreement.
UNIVERSAL PAYMENT ORDER (UPO) 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: a natural person using payment services as a payer or a payee or both, who uses digital banking, the e-Notifications portal, or the mobile wallet and who is party to a Consumer Payment Service Agreement with the Bank.
USERNAME: a randomly selected sequence of characters set by the Bank that does not change.
SAVER: a natural person who opens a savings account with the Bank.
SAVINGS ACCOUNT: an account through which, by request of the account holder, the Bank makes cash deposits, cash disbursements, internal cash transfers to savings products, deposits, and other accounts held with the Bank.
LEGALLY RESIDENT IN THE EUROPEAN UNION means that a natural person has the right to reside in a Member State based on EU or national law, which includes consumers without a permanent address and asylum seekers based on the Geneva Convention of 28 July 1951 Relating to the Status of Refugees and the Protocol of 31 January 1967 to the Convention and other international treaties governing the status of refugees and asylum seekers.
LEGAL GUARDIAN: natural person whose right to represent is based on the law (e.g. parents of a minor).

3 TRANSACTION ACCOUNTS

3.1 Opening a transaction account

The Bank will open a transaction account (TA) based on the parties entering into a Consumer Payment Service Agreement ("Agreement" or "Consumer Payment Service Agreement). This is to clarify that the decision to open a transaction account constitutes a business decision of the Bank, with the Bank having the right to reject the onboarding of a private individual due to its business policy.

The user can begin using the transaction account on the first business days following the account opening date other than in cases where the account is opened via electronic identification referred to in subsection 3.1.1. of these T&Cs. If an account is opened is opened via electronic identification, the user can begin using the account subject to terms stipulated by subsection 3.1.1. of these T&Cs.

The user is issued a Visa debit card to use their transaction account in the manner stipulated by subsection 3.6.3 of these T&Cs.

The Bank reports data on the transaction account to the transaction account register, which is a single database of data and records of transaction accounts in the Republic of Slovenia, in accordance with applicable regulations.

A transaction account held by a user who has the status of consumer cannot be used for payment services associated with gainful activity.

3.1.1 Opening a transaction account via electronic identification (using the mBank@Net app)

The Bank will enter into the Agreement and open a transaction account based thereon without the user being present by having the user undergo electronic identification via the mBank@Net app, subject to the user complying with the following requirements:

- The user has not kept a transaction account with the Bank in the last 12 months;
- The user is older than years of age;
- The user is a citizen of the Republic of Slovenia;
- The user keeps permanent and temporary residence in the republic of Slovenia;
- The user has valid personal ID with a biometric photo (personal ID card or Slovenian driving licence showing the address of residence);
- The user has an active mobile phone number from a Slovenian mobile provider;
- The user is a tax resident of the Republic of Slovenia only.

The Bank carries out electronic identification in the manner stipulated by subsection 7.5. of these T&Cs.

A user who meets the terms referred to above can open one of the following accounts or bundled offers via the mBank@Net mobile app:

- Komplet Bundle;
- Ekstra Bundle;
- Personal Plus Account;
- Youth Bundle;
- Prepaid Net Account.

The Bank does not charge the user is any remote contracting fees when opening a transaction account and entering into the agreement remotely.

Remote contracting means that the Bank and the user enter into an agreement remotely without the parties being present in person at the same time until and including the moment when the agreement takes effect. The Bank will open a transaction account in accordance with these T&Cs.

If the Agreement is entered into remotely (i.e. the Agreement is entered into via the mBank@Net app), the user has the right to communicate their intent to withdraw from the Agreement without having to provide a reason for their decision or pay a contractual penalty, provided they do so within fourteen (14) days of the da when the Agreement was entered into and in accordance with the provisions of the valid Consumer Payment Service Agreement. If the user withdraws from the Agreement within the timeline referred to above, the Bank shall have the right the charge the user only a proportional part of the fee for services rendered.

The Bank shall have discretion to decide on whether to open an account.

Parallel to opening the account, the user's access to the digital bank are activated as well. The client is provided with their username needed to log in via SMS, whereas the user can set their open personal password during the personal account opening process.

3.2 Transaction account types and bundled offers

The use of respective transaction account types is governed by the provisions of section 3 of these T&Cs in its entirety unless otherwise provided in the relevant subsections of this section.

3.2.1 Private individual transaction account

A private individual transaction account can be opened by a user who turned 15 years of age.

The Bank provides the following services as part of the private individual transaction account: all types of payment services, use of Visa debit card, Visa prepaid card, Visa charged card, use of standing order or SEPA Direct Debit, digital banking, SMS notifications about card-based account transactions, notifications about account activity, use of mobile wallet and Flik, and authorized overdraft.

If the account user has not yet reached legal age, the Bank does not provide the account overdraft service and Visa charged card.

3.2.2 Payment account with basic features

The Bank will open a payment account with basic features for a user who is legally resident in the European Union even if they do not have a permanent address and is an asylum seeker, and for a user whose application for a residence permit was denied, however, whose expulsion is not possible due to legal or factual reasons. This right applies regardless of the user's place of residence.

A payment account with basic features allows the user to use the following services: services needed to open, manage, and close the payment account, services to deposit cash to the payment account, services to withdraw cash from the payment account in the European Union at a teller's desk or ATM during or outside of the bank's business hours, domestic and cross-border direct debits, domestic and cross-border payment card-based payment transactions, including payments via digital banking, digital banking, domestic and cross-border credit transfers, including standing orders, at terminals, teller's desks and via the digital bank.

As part of the payment account with basic features services the Bank provides a total of eight (8) free-of-charge domestic and cross-border SEPA direct debits and domestic and cross-border credit transfers, including standing orders, at terminals, teller's desks and via digital bank per month. The Bank charges the user for every additional transaction and other services in accordance with the applicable Fee List.

The Bank does not provide authorized overdraft, credit card-based transaction or charge card-based transaction services on the payment account with basic features.

Cash and non-cash transactions on the payment account basic features are available only in domestic currency.

If the user opened a payment account with basic features for recipients of social transfers and the user no longer receives social transfers to their account, the Bank can transform the account into a regular payment account with basic features. This causes a change of the fee charged for the management of the payment account with basic features, as stipulated by the Fee List. If the user does not agree with the change, they can terminate the agreement in accordance with section 3.14 of these T&Cs.

The Bank can unilaterally terminate the Consumer Payment Service Agreement based on which it opened a payment account with basic features for the users only of one of the below conditions have been met:

1. The user has been intentionally using the payment account with basic features for unlawful purposes;
2. There have been no transactions on the payment account with basic features for more than twenty-four (24) consecutive months;
3. The user provided inaccurate information to obtain the right to a payment account with basic features and would not have obtained this right based on accurate data;
4. The user is no longer legally resident in the EU;
5. The user later opens a payment account with another bank to use services referenced in the second paragraph of this subsection;
6. The user breaches or has breached in the last three (3) years a contractual obligation owed to the Bank;
7. Under terms to terminate the agreement stipulated by another law.

If the Bank terminates the Agreement based on point 2, 4, or 5 of the previous paragraph of this subsection, it shall notify the user in writing and free of charge at least two (2) months prior to the termination taking effect about the causes for termination unless such disclosure is prohibited based on other regulations. If the Bank terminates the Agreement based on point 1, 3, or 6 of the previous paragraph of this subsection, the Agreement is terminated with immediate effect.

The Bank shall have the right to appeal against the Bank's decision to terminate the Agreement in the manner provided in section 7.10 of these T&Cs. The user shall also have the right to notify the Bank of Slovenia on the termination of the framework agreement to access a payment account with basic features.

3.2.3 Prepaid (Net) account

A prepaid account can be opened by a user who turned 15 years of age.

A prepaid account is intended to be used exclusively for Visa prepaid card payments. Services available with a prepaid account include cash deposits, withdrawals, payment transactions, standing orders (internal transfers), digital banking, SMS notifications about Visa prepaid card transactions, notifications about account activity, and use of mobile wallet. The account cannot be used for regular incoming payments of salary, pension, or scholarship.

The Bank does not provide Visa debit card, Visa charge card, SEPA Direct Debits, authorized overdrafts, or Flik services on the prepaid account.

The Bank shall have the right to change the prepaid account into a different transaction account type at any time if the user uses the account for incoming salary, pension, scholarship, or other regular incoming payments. If the user does not agree with the change of transaction account, they can terminate the Agreement in accordance with section 3.14 of these T&Cs.

3.2.4 Savings transaction account

A savings transaction account is intended exclusively for savings.

The following services are available on the savings transaction account: cash deposits, cash withdrawals, money transfer to a different account, standing orders (internal transfers), digital banking, and account activity notifications.

The following services are not available on the savings transaction account: use of Visa debit and prepaid card, charge card-based payment transactions, SEPA direct debits, SMS notifications about card-based payment transactions or overdraft, mobile banking, and Flik.

The Bank can convert the savings transaction account into a type of transaction account for which the user meets the terms if the user does not begin to receive incoming salary, pension, scholarship or other incoming payments. If the user does not agree with the change of the type of transaction account, they can terminate the agreement in accordance with section 3.14 of these T&Cs.

The Bank no longer opens new savings transaction accounts.

3.2.5 Election account

An election account can be opened by a user of legal age who is a Slovenian citizen for purposes of banking during an election campaign, whereby they are required to declare which elections or referendum they for which they are organizing a campaign.

The following services are available on an election account: all types of payment services, use of Visa debit card, digital banking, SMS notifications about card-based payment transactions, account activity notifications, mobile wallet, and Flik.

The following services are not available on an election account: overdraft, Visa charge card, Visa prepaid card, standing orders, and SEPA direct debits.

An election account cannot be converted into a different type of account. Similarly, a pre-existing account cannot be converted into an election account.

Data about accounts used for election campaigns are reported to the public part of the Transaction Account Register. The account user shall close the account by latest within four months after the date of voting. In the opposite case, the Bank will terminate the account after four months have passed since the date of voting in accordance with section 3.14 of these T&Cs.

3.2.6 Bundled offers

A bundled offer is a set of banking products in the extent outlined in these T&Cs for respective types of bundles that the bundle holder uses for a single monthly fee. The single fee for the use of services in the bundle may be subject to change in case of changes to the Fee List.

The Bank makes services from the bundle available to the user if so agreed by the user and the Bank.
The user can forgo a service that is included in the bundled offer, however, will still be charged the full fee set for the relevant type of bundle. If the user of a bundled offer wishes to use additional services as well, they need to pay the relevant fees in accordance with the applicable Fee List.

The Bank shall have full discretion to remove or change any service in a particular bundle. The user will be notified thereof in the manner provided in section 7.12 of these T&Cs.

3.2.6.1 Youth Bundle

The Youth Bundle includes the following services, subject to terms to use respective services based on the bundle holder's age, for a single monthly fee provided by the applicable Fee List:

- Transaction account management;
- First issue and regular replacements of Visa Debit card for the card holder;
- Digital banking;

- Security SMS notifications for Visa Debit card payments (for the card holder);
- Five (5) cash withdrawals per month using the Visa Debit card for the card holder at ATMs of other banks in Slovenia and EU countries where the local currency is EUR, SEK in RON (any fees charged by the ATM owner need to be verified at withdrawal).

The Youth Bundle is available to persons up to 27 years of age, in the manner and subject to the following terms:

a) Opening a bundle for a person up to 15 years of age:

The Youth Bundle can be opened on behalf of a person up to 15 years of age ("child") by one or both parents together as the legal guardians or a guardian whose right to open a bundle is based on a decision of the competent authority.

A child cannot manage the bundle and use the balances on the transaction account themselves. This is done on the child's behalf by their legal guardian who opened the bundle or a guardian. The legal guardian who did not open the bundle on the child's behalf may file a request during the term of the Agreement to manage the bundle and use balances on the transaction account, which can be done only with the consent of the legal guardian who opened the bundle. The Bank will issue a Visa Debit card by request only to the persons authorized to manage the bundle and use the balances on the transaction account in the manner described above.

The Bank can issue a Visa Debit card to the child by request of the legal guardian who opened the bundle or a guardian, thereby allowing them to use the balances on the transaction account. If, aside from the legal guardian, the balances on the transaction account are used by the child as well, the legal guardian who opened the bundle with the Bank guarantees by signing the Consumer Payment Services Agreement that they will pay the Bank any and all valid and past due debts arising from the child using the balances on the transaction account.

The following services are available with the Youth Bundle for persons up to 15 years of age: use of Visa Debit and Prepaid card, cash deposits and withdrawals, payment transactions, standing orders, SMS notifications about card-based payment transactions, account activity notifications, use of mobile wallet, and Flik.

The following services are not available with the Youth Bundle for persons up to 15 years of age: overdrafts, digital banking, SEPA direct debits, and charge card-based payment transactions.

The legal guardian or guardian shall not use the Youth Bundle to make payment transactions for their own purposes.

b) Opening a bundle for a person between 15 and 18 years of age:

A person between 15 and 18 years of age ("underage user") can open the Youth Bundle either alone, or have the bundle opened for them on their behalf by one or both parents together as the legal guardians or a guardian whose right to open a bundle is based on a decision of the competent authority, on condition that the underage user is not in an employment relationship and has the status of full high school or university student, which they prove by presenting valid personal ID and valid certificate of enrolment, high school student card, or university student card.

If an underage person between 15 and 18 years of age opened the bundle themselves, balances on the account may be used by the underage person themselves or by their authorized person, whereby transactions executed by the bundle holder or authorized persons are capped at EUR 1,000.00 each. If the accountholder wishes to withdraw more funds or execute a transaction on the account that exceeds this threshold or use the balances on the account without restrictions, they need written consent of one of the legal guardians. Consent applies only to the accountholder (underage person), however, not to any authorized account users, who can still execute transactions only up to EUR 1,000.00. If a parent is authorized to use the child's account, they can use the account without restrictions.

If the bundle for a person between 15 and 18 years of age was opened by a legal guardian, the account can only be used by the legal guardian. If the underage person wishes to use the balances on the account, they need written consent of one of the legal guardians. An underage person who presents a bank card can make a withdrawal or execute a transaction in a branch office alone, without a legal guardian, however, the transaction is capped at the amount of the daily debit card limit applicable to cash withdrawals at ATMs.

The legal guardian can provide consent when opening the account or at any time later in person at a Bank branch office. Consent of the legal guardian can be delivered by the underage person as well, whereby the consent needs to be notarized. Consent shall be valid until revoked by the legal guardian.

If, aside from the legal guardian, the balances on the transaction account are used by the underage person as well, the legal guardian who opened the bundle with the Bank guarantees by signing the Consumer Payment Services Agreement that they will pay the Bank any and all valid and past due debts arising from the underage person using the balances on the transaction account.

The legal guardian loses the right to manage the bundle in use balances on the underage person's transaction account once the latter gains full capacity to contract.

The underage user can authorize third parties to use the bundle and balances on the transaction account.

The following services are available with the Youth Bundle for persons between 15 and 18 years of age: use of Visa Debit card, use of Visa Prepaid card, cash deposits and withdrawals, payment transactions, standing orders and SEPA direct debits, digital banking, SMS notifications about card-based payment transactions, account activity notifications, use of mobile wallet, and Flik.

The following services are not available with the Youth Bundle for persons between 15 and 18 years of age: overdrafts and charge card-based payment transactions.

The legal guardian or guardian shall not use the Youth Bundle to make payment transactions for their own purposes.

c) Opening a bundle for a person between 18 and 27 years of age:

A person between 18 and 27 years of age ("legal-age user") can open the Youth Bundle alone, on condition that they are not in an employment relationship and has the status of full high school or university student, which they prove by presenting valid personal ID and valid certificate of enrolment, high school student card, or university student card.

The legal-age user shall meet the terms provided in the previous paragraph throughout the term of the contractual relationship. The Bank can request at any time during the term of the contractual relationship that the legal-age user provide proof of meeting these terms. If the legal-age user does not provide the documents referred to in the previous paragraph by request of the Bank, it shall be understood that they do not meet the terms, and the Bank will act in accordance with the fourth paragraph of this section.

The following services are available with the Youth Bundle for persons between 18 and 27 years of age: all types of payment services, use of Visa Debit card, use of Visa Prepaid card, standing orders and SEPA direct debits, digital banking, SMS notifications about card-based payment transactions, account activity notifications, use of mobile wallet, and Flik, and regular overdrafts.

Once the user has turned 27, the Youth Bundle is converted into the Retail Transaction Account. The Bank will convert the Youth Bundle into the Retail Transaction Account even before the user has turned 27 if it finds that a legal-age user is in an employment relationship or that their high school or university student status has ended. If the user does not agree with the change of the type of bundled/transaction account, they may cancel the agreement in accordance with section 3.14 of these T&Cs.

3.2.6.2 Personal Plus Account

A Personal Plus Account can be opened by a user who turned 15 years of age.

The Personal Plus Account includes the following services for a single monthly fee that is provided by the applicable Fee List:

- Transaction account management;
- First issue and regular replacements of Visa Debit card,
- Onboarding and management of digital bank.

The Bank can grant a Personal Plus Account user of legal age a regular overdraft of EUR 400.00 or an extraordinary overdraft of up to EUR 10,000, provided the user meets the terms.

The following services are available with the Personal Plus Account: all types of payment services, use of Visa Debit card, use of Visa Prepaid card, use of Visa charge card, standing orders and SEPA direct debits, digital banking, SMS notifications about card-based payment transactions, account activity notifications, overdrafts, use of mobile wallet, and Flik.

3.2.6.3 Komplet Bundle

A Komplet Bundle can be opened by a user of legal age who opens or keeps a Retail Transaction Account with the Bank.

The Komplet Bundle includes the following services for a single monthly fee that is provided by the applicable Fee List:

Daily banking benefits:

- Transaction account management;
- First issue and regular replacements of Visa Debit card for the cardholder:
- Security SMS notifications for the Visa Debit card for the cardholder;
- Onboarding and management of digital bank;
- Domestic and cross-border payments via digital bank for non-urgent and instant payments up to and including EUR 50,000 and non-urgent payments in SEK up to value equivalent of EUR 50,000;
- Five (5) executed SEPA direct debits per month;
- Unlimited number of standing orders;
- Account activity notifications;
- Use of mobile wallet and Flik.

Investment banking benefits:
- 25% off on entry and distribution fees for mutual funds in the Bank's product range for one-time payments;
- Annual retail trading account management fee.

General and other benefits:
- Lower interest rate on housing loans (in accordance with the valid Decision on Interest Rates);
- Lower safety deposit box rental fees;
- Discount on home insurance premium.

The Bank can grant a legal-age user of the Komplet Bundle a regular overdraft of EUR 400.00 or an extraordinary overdraft of up to EUR 10,000.00 without origination fees, provided the user meets the terms.

3.2.6.4 Extra Bundle

An Extra Bundle can be opened by a user of legal age who opens or keeps a Retail Transaction Account with the Bank.

The Extra Bundle includes the following services for a single monthly fee that is provided by the applicable Fee List:

Daily banking benefits:
- Transaction account management;
- First issue and regular replacements of Visa Debit card for the cardholder;
- First issue and regular replacements of Visa (virtual) Prepaid card for the cardholder;
- Annual charge card membership fee for the cardholder;
- Security SMS notifications for Visa Debit and Visa (virtual) Prepaid card and Visa charge card payments for the cardholder;
- Five (5) cash withdrawals per month using the Visa Debit card for the card holder at ATMs of other banks in Slovenia and EU countries where the local currency is EUR, SEK in RON (any fees charged by the ATM owner need to be verified at withdrawal);
- Onboarding and management of digital bank;
- Domestic and cross-border payments via digital bank for non-urgent and instant payments up to and including EUR 50,000 and non-urgent payments in SEK up to value equivalent of EUR 50,000;
  Ten (10) executed SEPA direct debits per month;
- Unlimited number of standing orders;
- Account activity notifications;
- Use of mobile wallet and Flik.

Investment banking benefits:
- 25% off on entry and distribution fees for mutual funds in the Bank's product range for one-time payments;
- Annual retail trading account management fee.

General and other benefits:

- Lower interest rate on housing loans (in accordance with the valid Decision on Interest Rates);
- Lower safety deposit box rental fees;
- Discount on home insurance premium.

The Bank can grant a legal-age user of the Extra Bundle a regular overdraft of EUR 400.00 or an extraordinary overdraft of up to EUR 10,000.00 without origination fees, provided the user meets the terms.

3.2.6.5 Premium Bundle

A Premium Bundle can be opened by a user who, aside from the basic terms to use a transaction account, meets additional terms to open a Premium Bundle.

The terms to open a Premium Bundle are as follows (changes in force as of 1 January 2026):
- The bundle holder's regular cash inflow over the last six months was at least EUR 2,500 for at least 5 months, or
- The bundle holder keeps at least EUR 50,000 in deposits, savings, average transaction account balance, assets in mutual funds distributed by the Bank, securities on a trading account with the Bank, or a combination of various investments, or any combination of the above products and accounts.

Sole traders of company owners who do not meet the above terms shall meet the following criteria: annual earnings over EUR 0,5M, company has been in business for at least two years, the company runs at least 50% of its business through an account with the Bank, and other terms according to the Bank's internal rules.

The Premium Bundle includes the following services for a single monthly fee that is provided by the applicable Fee List:

Daily banking benefits:
- Transaction account management;

- First issue and regular replacements of Visa Premium Debit card for the cardholder and Visa Debit cards for their authorized users;
- First issue and regular replacements of Visa (virtual) Prepaid card for the cardholder and their authorized users;
- Annual Visa Premium charge card membership fee for the cardholder and their authorized users;
- Security SMS notifications for Visa Debit card, charge card, and Visa (virtual) Prepaid card payments for the cardholder and their authorized users;
- Cash withdrawals with Visa Debit card on the Bank's ATMs and ATMs of other banks in Slovenia and globally (any fees charged by the ATM owner need to be verified at withdrawal);
- Individually agreed daily ATM cash withdrawal limit for the Visa Premium Debit card for the cardholder and Visa Debit card for their authorized users;
- Onboarding and management of digital bank;
- Domestic and cross-border payments via digital bank for non-urgent and instant payments up to and including EUR 50,000 and non-urgent payments in SEK up to value equivalent of EUR 50,000;
- Unlimited SEPA direct debits per month;
- Unlimited number of standing orders;
- Account activity notifications;
- Use of mobile wallet and Flik,
- Collective card insurance (as of 1 January 2026).

Investment banking benefits:
- Selection and presentation of investment services based on the customer's choice that are prepared in cooperation with investment experts;
- Consultation with an expert on financial instrument investment opportunities (2 hours per year);
- At least one Financial Report per year;
- 75% off on entry and distribution fees for mutual funds in the Bank's product range for one-time payments (change effective as of 1 January 2026);
- Annual retail trading account management fee;
- 30% off on the Bank's brokerage fee for financial instrument trading (orders made by phone and in person);
- 0.20% brokerage fee (no fee minimum) for trading via digital bank.

General and other benefits:
- Personal banker;
- Separate customer premises;
- Priority treatment and pre-agreed meetings;
- Remote services;
- Lower interest rate on consumer loans (in accordance with the valid Decision on Interest Rates)
- Lower interest rate on housing loans (in accordance with the valid Decision on Interest Rates);
- 50% off on housing loan origination fees;
- Lower safety deposit box rental fees;
- Various statements and records by request of the customer;
- Option to attend various Premium events (Premium experiences);
- Discount on home insurance premium;
- Exclusive Visa benefits.

The Bank can grant a user of the Premium Bundle a regular overdraft of EUR 2,000.00 or an extraordinary overdraft of up to EUR 15,000.00 without origination fees, provided the user meets the terms.

To use the Premium Banking service, users can rely on the assistance of a personal banker every business day during the branch office's business hours, which are posted on the Bank's website, or by phone every business day between 8:00 and 20:00. The personal banker is the relationship manager of the Premium Bundle user. Their task is to coordinate the user's financial transactions in the Bank and report to the user upon their request on the balance and movement of funds, investment opportunities, and changes. The personal banker produces the user's financial plan and monitors its delivery.

In case of unexpected and shorter absence of the personal banker, the Bank will make all the necessary arrangements to ensure unimpeded delivery of the Premium Banking service.

The Bank can terminate the Premium Bundle, or replace it with a different type of bundled offer, at two (2) months' notice if the user does not meet the Bank's internal rules for this bundle. The Bank acts in the bundle termination process as outlined in section c), subsection 3.14. The user can enter into a different bundled offer arrangement with the Bank that they meet the terms for.

Card insurance (as of 1 January 2026)

By signing the Bundled Transaction Account Agreement, the customer, a Premium Bundle holder, acknowledges and expressly agrees to become a party to the Premium Banking collective card insurance contract for private individuals ("Insurance Contract") as a policyholder. The Insurance Contract is made between the Bank and Zavarovalnica Sava d.d., Ulica Eve Lovše 7, 2000 Maribor ("Insurance Company"). The customer (policyholder) declares to have been made aware

prior to becoming a party to the insurance arrangement of objective information about the insurance, the terms of the collective card insurance that are an integral part of the Insurance Company, the information on personal data protection and processing of Sava insurance company (more information available on the Insurance Company's website at https://www.zav-sava.si/o-nas/zasebnost/), and confirms that the insurance meets their needs.

The insurance coverage for the policyholder under the Insurance Contract takes effect at 24:00 on the day when the policyholder becomes a Premium Bundle user. The insurance coverage for the policyholder ends as of the day when they are no longer a Premium Bundle user or as of the date of termination of the Insurance Contract. Insurance coverage for the relevant card is also terminated if the card is terminated due to reasons that include expiration of the card, removal of the card, blocking of the card.

The substance of insurance as well as the procedure to claim rights under the insurance arrangement are outlined in the terms of collective card insurance that the customer, as a policyholder, is notified of when signing the Bundled Transaction Account Agreement.

3.2.6.6 Private Banking Bundle

A Private Banking Bundle can be opened by a user who, aside from the basic terms to use a transaction account, meets additional terms to open a Private Banking Bundle.

Private Banking terms:
- The holder's average transaction account balance over the last six months was at least EUR 250,000; or
- The holder kept deposits or savings of at least EUR 250,000 over the last six months; or
- The holder keeps assets in mutual funds distributed by the Bank, securities on the trading account, or a combination of different investments of at least EUR 250,000; or
- The holder keeps at least EUR 250,000 in assets in any combination of the above products; or
- The holder provides at least EUR 250,000 in assets in any combination of the above products within six months of opening the Private Banking Bundle.

The Private Banking Bundle includes the following services for a single monthly fee that is provided by the applicable Fee List:

Daily banking benefits:
- Transaction account management;
- First issue and regular replacements of Visa Private Banking Debit card for the cardholder their authorized users;
- First issue and regular replacements of Visa (virtual) Prepaid card for the cardholder and their authorized users;
- Annual Visa Private Banking charge card membership fee for the cardholder and their authorized users;
- Security SMS notifications for Visa Private Banking Debit card, charge card, and Visa (virtual) Prepaid card payments for the cardholder and their authorized users;
- Cash withdrawals with Visa Debit card on the Bank's ATMs and ATMs of other banks in Slovenia and globally (any fees charged by the ATM owner need to be verified at withdrawal);
- Individually agreed daily ATM cash withdrawal limit for the Visa Private Banking Debit card for the cardholder and their authorized users;
- Onboarding and management of digital bank;
- Domestic and cross-border payments via digital bank for non-urgent and instant payments in EUR and non-urgent payments in SEK up to value equivalent of EUR 50,000;
- Unlimited SEPA direct debits per month;
- Unlimited number of standing orders;
- Account activity notifications;
- Use of mobile wallet and Flik.

Investment banking benefits:
- Financial advice;
- Development of investment ideas based on the customer's wants and needs;
- At least one Financial Report per year;
- Report on investments subject to quarterly advice with the option of individual overview of investments in cooperation with the customer;
- Consultation with investment expert (four hours per year);
- Entry and distribution fees for mutual funds in the Bank's product range for one-time payments;
- Annual retail trading account management fee;
- 50% off on the Bank's brokerage fee for financial instrument trading (orders made by phone and in person);
- 0.20% brokerage fee (no fee minimum) for trading via digital bank.

General and other benefits:
- Private banker;
- Personalized, priority, and discreet treatment;

- Remote services;
- Safety deposit box rental;
- Statements and records by request of the customer;
- Exclusive Visa benefits;
- Exclusive experiences at culinary, sports, cultural, and educational events;
- Discount on home insurance premium;
- Travel insurance and card and personal item protection insurance;
- The private banker collects tax-related data using standardized OTP banka templates;
- Transaction sheets for securities sales at OTP banka;
- Option to include family members (up to 27 years of age) into the Private Banking service.

The Bank can grant a user of the Premium Bundle a regular overdraft of EUR 3,500.00 or an extraordinary overdraft of up to EUR 20,000.00 without origination fees, provided the user meets the terms.

The user can forgo a service that is included in the Private Banking Bundle, however, will still be charged the full fee set for this type of bundle. If the user of the Private Banking Bundle wishes to use additional services as well, they need to pay the relevant fees in accordance with the applicable Fee List.

The private banker is the relationship manager of the Private Banking Bundle user. Their task is to coordinate the user's financial transactions in the Bank and report to the user upon their request on the balance and movement of funds, investment opportunities, and changes. The private banker produces the user's financial plan and monitors its delivery and provides investment advice to the user upon request. To use the Private Banking service, users can rely on the assistance of their private banker every business day during the branch office's business hours, which are posted on the Bank's website, or by phone even outside of business hours to seek advice and information. In this case, the Bank will deliver the services that can be provide only within the Bank's business hours in the shortest possible time after the beginning of business hours and within timelines provided for the relevant services.

Advisory services regarding the recommended structure of the customer's portfolio consist of personal recommendations given to the customer regarding the recommended structure of their portfolio and consider the customer's financial position, family and other personal situation, expected term of investment, purposes given the use of financial assets, the customer's risk profile and risk appetite, hedging arrangements, etc. The customer is independent in taking a decision for any investment based on the advice.

The Bank undertakes to perform the work under the contract in a reasonable, professional and quality manner and with the diligence of a good expert.
The Bank can deny the customer the service if it makes the assessment that the transactions are inappropriate, if the customer's banking is counter to the Bank's policy, if it believes that a particular transaction is not to the benefit of the customer/Bank, and if providing the service would be counter to the law.
The Bank does not guarantee the results of any transaction that the customer executes by advice of the Bank and shall not be liable for any damage suffered by the customer or third party in relation to such an executed transaction unless the damage was caused by the Bank's wilful actions or major negligence on its part, whereby the Bank shall be liable only for direct damage and not for any lost earnings, profit, or any other type of indirect damage.

In case of unexpected and shorter absence of the private banker, the Bank will make all the necessary arrangements to ensure unimpeded delivery of the Private Banking service.

If the user cancels the Private Banking Bundle, the user's family members who were onboarded when the Private Banking Bundle was opened or later during the term of the Private Banking Bundle shall be removed from the bundle as well.

The Bank can terminate the Private Banking Bundle, or replace it with a different type of bundled offer, at two (2) months' notice if the user does not meet the Bank's internal rules for this bundle. The Bank acts in the bundle termination process as outlined in section c), subsection 3.14. The user can enter into a different bundled offer arrangement with the Bank that they meet the terms for.

Card insurance

By signing the Bundled Transaction Account Agreement, the customer, a Private Banking Bundle holder, acknowledges and expressly agrees to become a party to the Private Banking collective card insurance contract for private individuals ("Insurance Contract") as a policyholder. The Insurance Contract is made between the Bank and Zavarovalnica Sava d.d., Ulica Eve Lovše 7, 2000 Maribor ("Insurance Company"). The customer (policyholder) declares to have been made aware prior to becoming a party to the insurance arrangement of objective information about the insurance, the terms of the collective card insurance that are an integral part of the Insurance Company, the information on personal data protection and processing of Sava insurance company (more information available on the Insurance Company's website at https://www.zav-sava.si/o-nas/zasebnost/), and confirms that the insurance meets their needs.

The insurance coverage for the policyholder under the Insurance Contract takes effect at 24:00 on the day when the policyholder becomes a Private Banking Bundle user ("Private Banking") or on 31 August 2024 at 24:00 if the policyholder became a Private Banking Bundle user ("Private Banking") before 1 September 2024. The insurance coverage for the policyholder ends as of the day when they are no longer a Private Banking Bundle user ("Private Banking") or as of the

date of termination of the Insurance Contract. Insurance coverage for the relevant card is also terminated if the card is terminated due to reasons that include expiration of the card, removal of the card, blocking of the card.

The substance of insurance as well as the procedure to claim rights under the insurance arrangement are outlined in the terms of collective card insurance that the customer, as a policyholder, is notified of when signing the Bundled Transaction Account Agreement.

Travel insurance with travel assistance for Private Banking bundle holders

By signing the Bundled Transaction Account Agreement, the customer, a Private Banking Bundle holder, acknowledges and expressly agrees to become a party to the Travel Insurance and Travel Assistance product – Extended+ package, made with Zavarovalnica Sava d.d., Ulica Eve Lovše 7, 2000 Maribor ("Insurance Company"). The policyholder declares to have been made aware prior to becoming a party to the insurance arrangement of objective information about the insurance and that they and, in case the insurance extends to family members as well, their family members have permanent or temporary residence in the Republic of Slovenia. By completing the application, the customer may opt for single or family insurance. The customer agrees with publicly available general terms and conditions of insurance governing the insurance policy between the Bank and the Insurance Company and confirms that the insurance meets their needs.

Travel insurance with travel assistance – Extended+ package, Global Coverage, includes the following services and coverages with the sum insured of EUR 100,000:*

- Assistance Call Centre service;
- Outpatient clinic costs;
- Dental service costs up to EUR 300;
- Hospital costs;
- Non-urgent transport to healthcare facility up to EUR 50;
- Urgent transport to healthcare facility and relocation of policyholder during treatment;
- Transport of policyholder to Slovenia after end of treatment;
- Return of underage children;
- Visit by policyholder in case of hospitalization;
- Unexpected return of policyholder to Slovenia;
- Transport of policyholder's remains to Slovenia;
- Refund of urgent costs in case of missed flight;
- Refund of urgent costs associated with loss of luggage during air travel;
- Refund of costs associated with new government-issued personal ID in case of lost or stolen documents up to EUR 50;
- Personal liability insurance.

*Maximum sum insured to be disbursed per each insurance event. Annual aggregate for all insurance events per policyholder is EUR 200,000,

The insurance coverage for the policyholder takes effect at 0:00 on the day after opening a Private Banking Bundle. The insurance coverage for the policyholder ends as of the day when they are no longer a Private Banking Bundle user. The insurance coverage is not valid in Slovenia and/or the country in which the policyholder keeps permanent or temporary residence.

In accordance with the General Terms and Conditions for TZA Insurance, in case of an event covered by the insurance, the policyholder shall immediately (before they organize help themselves) call or notify the 24-hour call centre of Zavarovalnica Sava d.d. that will organize assistance.

Call Centre	Country calling code	Local calling code	Telephone number and email
TBS Team 24 d.o.o.	+386	2	Calls from Slovenia: 080 19 21 Calls from abroad: 618 05 20 (charges borne by policyholder) Email: opsmed@tbs-team24.com

The policyholder shall provide the following details when calling the Call Centre:

- Name, surname, and address of policyholder,
- Location of policyholder and telephone number and any address where the policyholder can be reached,
- Brief description of the issue and type of assistance requested,
- Proof that travel abroad has not lasted for more than ninety-two (92) consecutive days,
- Any other additional documentation by request of Zavarovalnica Sava d.d.

Payment of the insurance guarantee is guaranteed for by Zavarovalnica Sava d.d. Any and all provisions and terms to exercise the insurance guarantee are provided in the applicable version of the General Terms and Conditions for TZA Insurance that are available to the policyholder at their private banker in OTP banka's Private Banking branch office, on the website of the Bank, or the website of Zavarovalnica Sava d.d. at https://www.zav-sava.si/sl-si/zavarovanja/potovanje/letno/.

3.3 Authorized users

The accountholder can authorize one or more persons to use the funds in their transaction account. An authorized user can be a natural person of legal age with full capacity to contract. The power of attorney needs to be made in writing and can be granted to execute a single action or as a general power of attorney.

If the transaction account has been opened on behalf of an accountholder who has been placed under guardianship by decision of the competent authority, the accountholder or guardian cannot authorize a third party to use the funds in their account.

The accountholder and the authorized person need to sign the power of attorney in the presence of the competent Bank employee, or the accountholder shall have their signature on the power of attorney notarized.

Persons authorized to use funds in the transaction account shall deposit their specimen signature with the Bank.

In case general power of attorney is granted, the authorized user can freely use the funds in the account within the available account balance unless otherwise provided by regulations, and can open deposits on behalf and for the account of the accountholder that authorized them. General power of attorney gives the authorized user the right to use the accountholder's funds and transaction account also via the digital bank, provided the authorized user keeps a transaction account with OTP banka. The authorized user can be issued their own Visa Debit card and is authorized to use payment services with all payment instruments (is free to choose the payment instrument).

The authorization to use funds in the transaction account does not include the right to extend further authorizations or to delegate an authorization to a third party, change the policyholder's basic data, which includes but is not limited to the address and contact details used to communicate with the accountholder, apply for an overdraft on the account, or the right to cancel the Consumer Payment Services Agreement or close the transaction account.

The power of attorney the user grants to a third party shall remain valid until:

- The Bank has been informed in writing that the power of attorney has been revoked (either by the user or the authorized user);
- The Bank has been informed in writing that the user or authorized user has died (by being provided with an official document). In case the authorized user dies, the accountholder shall notify the Bank thereof immediately. In case the accountholder dies, the authorized user shall be required to notify the Bank thereof and stop using the accountholder's transaction account immediately;
- The transaction account has been closed.

After the power of attorney has been revoked, SEPA direct debits, standing orders, and payment orders made by the authorized user during the term of the power of attorney shall remain valid.

Funds of a deceased accountholder can be used exclusively by their heirs based on a final decision on inheritance, which is why the Bank blocks the accountholder's account after receiving a notice that the accountholder has died until it has been provided with a final decision on inheritance. The Bank can release funds to cover funeral fees only based on a court decision. The Bank shall not be liable for any damages caused by the authorized user who continues to use the transaction account after the accountholder has or died or after power of attorney has been revoked if the Bank was not notified thereof in one of the ways referred to in the previous paragraph.

3.4 Transaction account management

The Bank manages the transaction account in local or foreign currency from the list of reference rates of the European Central Bank or the Bank of Slovenia. Currency exchange is executed in accordance with regulations and provisions of the Bank's rules.

The Bank undertakes to provide payment services to the user via the transaction account within the available transaction account balance. Transaction account balances are regarded as sight cash deposits at the bank that manages the transaction account.

If the transaction account balance is lower than the coverage due to any reason, this is regarded as unauthorized negative account balance.

3.5 Executing payment transactions

3.5.1 Receiving an order

The Bank executes a payment transaction once it is provided with a payment order, unless terms to reject the payment order are met. Payment orders need to be completed in accordance with regulations, payment system standards, and these T&Cs. A payment order shall include the following essential elements:

- payer's name and address;
- payer's IBAN;
- amount and currency of payment;
- payee's name and surname/title and address;
- payee's IBAN or account number; BIC or accurate address of 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.

It is understood that the Bank received a payment order once the payment order has been delivered to it in paper or electronic format or through agreed-on communication channels in one of the following ways:

- The payment order is delivered at a Bank counter;
- The payment order is delivered via the digital bank.

Using a payment instrument documented by the Bank proves to the Bank that the payer has approved the payment transaction.

If Bank receives a payment order is received 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, other than in case of an instant payment.

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 payer's request to the Bank is made in the form of a standing order or direct debit, it shall be deemed that the payment order was received on the execution date of the standing order or direct debit.

3.5.2 Verification of Payee

During the payment order initiation process and prior to confirmation, the Bank verifies with the payee's bank whether the payee's name and IBAN match.

In case of a mismatch or partial match, a message will appear for the user, alerting them that there is a chance that the money will not be transferred to the right payee. The user can disregard the alert and proceed with delivering the payment order to the Bank for execution The Bank shall have no liability in this case if the payment is made to the wrong payee.

If the user does not proceed with the confirmation of the payment order due to having received an alert about a mismatch or partial match, it shall be understood that they withdrew from initiating a payment order or money transfer. The user hereby acknowledges that the Bank will not store the data on the unconfirmed payment order because the payment order was not delivered to the Bank for execution.

The user shall verify the correct name and IBAN of the payer before making a payment order again.

3.5.3 Instant payments limit

In order to enhance the security of instant payments, the Bank allows the user to set limits on the execution of instant payments. The user can thus set up the following instant payments limits:

- Maximum amount of single instant payment,
- Daily instant payments limit.

The set limit applies to all instant payments initiated via the digital bank, in Bank branch offices, Pošta Slovenije branches, and the mobile wallet. The default daily instant payments limit for digital channel users is identical to the daily limit in the digital bank. The default daily limit for other users is EUR 15,000. The single instant payment limit shall not exceed the instant payments daily limit.
The user can change the limit themselves at any time at a Bank counter, via the digital bank, or by calling the Contact Centre.

3.5.4 Execution of domestic and cross-border instant payment

An instant payment is executed within 10 seconds of receipt of a complete payment order in the banking system. The payee's bank communicates to the payer's bank within this timeframe whether it has credited the funds to the payee's account or rejected the order.

After receiving feedback from the payee's bank, the Bank will notify the payer on the execution or rejection of the instant payment via the digital bank or at the Bank counter if the order was made at a Bank branch office. If an instant payment is rejected, the Bank will also immediately refund the funds to the payer's account.

Due to technical and other objective reasons, there is a chance that the Bank will not receive feedback from the payee's bank within 10 seconds. The Bank will also notify the payer in the manner referred to in the previous paragraph of the fact that it did not receive feedback on whether the payment order has been executed or not, and will refund the funds to the payer's account. The user hereby authorizes the Bank to re-authorize the funds on the payer's account for the amount of the instant payment for which the execution status is not known until the Bank has received feedback on the execution or rejection status of the instant payment. The Bank will make a final debit to the account immediately after receiving final feedback on the status of the order, provided the instant payment has been confirmed, whereas in cases where the instant payment is rejected, it will immediately release the authorization and make the funds available on the payer's account. The payer hereby agrees that the Bank may authorize the funds until it has received a message from the payee's bank and for no more than 24 hours. Once 24 hours have passed since the reauthorization of funds, the Bank will release the authorization and make the funds available on the payer's account irrespective of whether it has received information about the status of the order, and shall notify the payer thereof.

3.5.5 Execution of payment order

a) <u>By authorization of the user:</u>

The Bank will execute a payment order according to the payment transaction schedule attached hereto in the Appendix to these T&Cs if the following conditions are fulfilled:

- The Bank received the payment order in line with the Bank's payment schedule that is enclosed to these T&Cs as an integral part, provided there is sufficient account balance;
- The payment order is signed, completed in a legible manner (without corrections) and contains all requested data required under the first paragraph of subsection 3.5.1. of these T&Cs;
- The user is not subject to sanctions or does not meet the conditions laid down in paragraphs 3 and 4 of section 7.2. of these T&Cs (Sanctions);
- There are no regulatory or internal impediments or restrictions to execute 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. Receiving such a payment order does not yet trigger any rights or claims of third parties on the Bank.

If the payment order shows a future execution date, the Bank shall verify the conditions for the execution of the order on that day.

The user and the Bank can agree that payment orders shall be executed based on priorities set by the user, otherwise the Bank will execute in the order in which they were received by the Bank. In doing so, the Bank considers the priorities provided by law.

The Bank does not verify the purpose code and will forward it to the payee in the form as stated by the user.

The Bank shall not be liable for inappropriate processing of a payment transaction if the user or the authorised user does not use the payment purpose code corresponding to the actual purpose

In accordance with SEPA rules, a simultaneous transfer of the structured reference and the text showing 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 showing the payment purpose.

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

For a standing order or a SEPA 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). The Bank shall also have the right to reject an incoming payment or not verify the payee's account if the payee meets the criteria under paragraphs 3 and 4 of section 7.2 (Sanctions).

The Bank executes the payment order subject to fulfilment of terms provided in the first paragraph of this subsection. The Bank shall have no responsibility for the effects of the transactions between the user and the payee that serve as the basis for the initiation of the payment transaction. The user is responsible for decisions taken in connection with the conclusion of a transaction and for the credit rating assessment and other circumstances on the part of the payee. If the user initiates 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. The user shall have full and sole responsibility to make independent inquiries on their own regarding the financial instruments or other services that are the subject of their investment decision.

b) Without authorization of the user:
The Bank will execute a payment transaction without the authorization of the user or authorized user based on an executable enforcement order or any other decision issued by the competent authority in accordance with the legislation applicable at the time.

The Bank will charge the user a fee for the execution of the payment order in accordance with the Bank Fee List 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, via the digital bank, at a Post office counter).

3.5.5.1 Executing payment orders made via digital bank

Payments are executed in accordance with these T&Cs and the payment schedule attached to these T&Cs in the Appendix.

The Bank will execute the payment or transfer of funds on the date selected by the user, provided the account shows sufficient balance, the daily account spending or instant payments limit set by the accountholder has not been exceeded, and the account has not been blocked. Executed payments are shown under the Completed/executed requests tab.

If the account balance is too low or the daily account spending limit has been exceeded, the payment or transfer of funds will be executed once there is sufficient account balance, the daily account spending limit is still available, or by the latest future execution date selected (if payment delay dates have been selected in the digital bank). If sufficient account balance has not been provided until a certain date or the daily account spending limit is still exceeded, the payment or transfer of funds will not be executed and is moved to the Rejected requests tab.

With instant payments, the payment order is rejected immediately if the account balance is too low or the daily account spending or instant payments limit have been exceeded. The user can manage the instant payments limit themselves and can change it at any time via the digital bank, Contact Centre, or at a Bank counter.

Pending payments and transfer of funds are executed event if the user cancels the use of the digital bank before the payment execution date.

Payment via digital bank is equivalent to a written request or order made at a Bank branch office.

Electronic payment orders that the user submits to the Bank need to be completed according to payment operations standards. The user is responsible for the accuracy and integrity of data on the payment order. If a payer presents to the Bank for execution a paper-based payment order with a QR code, the Bank may forward to the payee and their bank only the information included in the QR code. The Bank shall not be required to verify whether the QR code matches other data in the payment order, other than the payee's name and IBAN.

The payment order shall be made out for execution on the same day or a future date (whereby it need not be a business day). The Bank accepts correctly completed payment orders every day and executes them in accordance with the payment schedule provided in the Appendix to these T&Cs, provided there is sufficient account balance to cover the payment, and the daily spending or instant payments limit have not been exceeded.

The Bank will charge the user a fee for the execution of the payment order via the digital bank in accordance with the Bank Fee List applicable at the time.

3.5.6 Rejection of payment order

The Bank can reject the execution of the payment order if any of the conditions for the execution specified in these T&Cs are 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 this is prohibited by other regulations.

With instant payments, the Bank can reject the execution of the payment order if it identifies sanctions-related risks.

The Bank will send the notification referred to in the first paragraph to the user or make it available to the user at the first opportunity and by latest within the deadline provided for the execution of the payment order in subsection 3.5.2.

The Bank can charge the user a fee for the payment rejection notice if the cause of the rejection is insufficient account balance or if the payment order was not completed in accordance with these T&Cs. The fee is provided in the applicable version of the Fee List.

3.5.7 Cancellation of payment order

The user can cancel the payment order at any time by:
- Revoking authorization to execute a payment transaction or batch of payment transactions;
- Requesting that the payment order be returned;
- Cancelling an electronic payment order;
- Revoking authorization for a standing order or direct debit.

Any payment transaction executed after the cancellation shall be considered unauthorised. The user can cancel the payment order no later than by the end of the business day preceding the payment date. The user cannot revoke an instant payment order because the Bank executes it immediately. In case of a mismatch or partial match of the payee's name and IBAN, the user can reject the payment order before the payment order is initiated (before it is delivered to the Bank for execution).

Notwithstanding the first paragraph of this subsection, the user cannot cancel a payment order once the payment order to execute a payment transaction became irrevocable, that is, once it has been received by the payee's bank. If the payment transaction is initiated by a payment initiation service provider, the payee, or the user through the payee, the user is not allowed to cancel the payment order once they have authorized the payment initiation service provider to initiate the payment transaction or once they gave their consent to execute the payment transaction to the credit of the payee.

Notwithstanding the above, in cases where the payment transaction is initiated by the payee by way of a SEPA direct debit, the user may cancel 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 expiration of the deadlines referred to in the third and fourth paragraph of this subsection, the user may cancel the payment order only in agreement with the Bank. The latter does not apply to instant payments. If the payment transaction is initiated by the payee or by the user through the payee, the cancellation of the payment order after the end of this deadline needs to be authorised by the payee as well.

The Bank may charge the user a fee for the cancellation of the payment order referenced in the previous paragraph in accordance with the Fee List applicable at the time.

3.5.8 Request to cancel executed payment order

A cancellation of an executed payment order may only be requested in the case of duplicated transaction, technical issues, or fraud. The user shall send the Bank a written request to cancel 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 refunded the amount only with consent of the payee. The amount refunded 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 cancellation from another bank, it shall notify the user (payee) of having received the payment cancellation request (consent). The user (payee) shall confirm or reject the request for cancellation in writing in eight (8) days. If the request is confirmed, the Bank shall refund the sum to the payer. If the request is rejected or the user does not respond to it, the Bank will not refund the payment.

3.5.9 Liability of the Bank and refund of payment transactions

a) <u>Liability of the Bank for unauthorized payment transaction:</u>
The Bank is liable to the user for having executed a transaction without the user's consent to execute (unauthorised payment transaction) in accordance with subsection 3.5.2 and 3.5.2.1 of these T&Cs. 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 no 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 fraud or a scam has been committed.

If an unauthorised payment transaction was debited to the user's payment account, the Bank shall revert 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 be relieved from liability to refund the sums of unauthorised payment transactions:
- If an unauthorised payment transaction was executed due to 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 unauthorised payment transaction was caused by the user committing fraud or because the user failed to meet their obligations in relation to the payment instrument wilfully or due to gross negligence;

- If the user submitted to the Bank a counterfeit or modified payment order;
- In the amount from the below paragraph covered by the user if the execution of an unauthorised payment transaction is the result of using a stolen or lost payment instrument or a payment instrument that was misused (if the user failed to protect 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, unless the loss, theft, or misuse could not have been discovered before the payment was made or the loss is the result of actions or failure to act by Bank employees. 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 refund 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 if 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 relieved of liability under this paragraph if the damage is the result of the user committing fraud or a scam.

b) Liability of the Bank for non-execution, incorrect execution, or late execution of a payment transaction initiated by the user:
If the Bank is liable for the non-execution and/or incorrect 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, revert the balance of the user's payment account to the balance as it would have been had the payment transaction not been executed incorrectly. The date of credit shall not be later than the date on which the amount was debited.

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.
If the payment transaction is credited to the payee's payment account, the appropriate sum shall be credited to the payee's payment account. The date of credit on 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 liable toward its user in case of a non-executed or incorrectly executed payment transaction or a payment transaction that was executed late also for the refund of the loss incurred by fees that the Bank charged to the user, whereas the user shall be entitled to interest only in case of an incorrectly executed payment transaction.

The Bank shall be relieved from liability to refund the sums of non-executed or incorrectly executed payment transactions or payment transactions executed late:
- 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;
- 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.

c) Liability for using unique identifier:
If the user provides the Bank with an incorrect unique identifier of the payee 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 incorrect 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 suffered by the user as a result of execution of falsified or modified payment orders.

.

d) Payment transaction refund in case of SEPA direct debits:
The user can request the refund of an executed direct debit by providing supporting documents within eight (8) weeks of the executed direct debit if the user authorized a direct debit without a specified sum of the direct debit and if the sum of the direct debit exceeds the sum that the user could have reasonably anticipated by considering the sums of past payment transactions, contractual terms, and other circumstances, as the case may be (does not apply to foreign exchange). The Bank may request of the payer to prove their eligibility to have the direct debit refunded. The Bank will refund the user the full sum of the payment transaction within ten (10) business days after receipt of the refund request or notify the user on having rejected the request and provide the cause of rejection. The user shall not be entitled to a refund of an executed direct debit if the user authorized the Bank to execute the transaction directly and the Bank or payee has communicated or made available in the agreed manner information about the future payment transaction at least four (4) weeks prior to the payment due date.

3.5.10 Use of funds

Funds in the transaction can be used only by the accountholder or a third party authorized by the accountholder. The user of funds is unlimited within the available balance unless otherwise provided by regulations.

If the transaction account holder is under guardianship, the guardian can use the funds in the transaction account based on a decision of the competent authority. The use of this account shall be consistent with the stipulations made in this decision.

The user (payee) can use the funds in their transaction account once the sum of the payment transaction has been credited to the Bank's account in accordance with the payment transaction execution schedule and once the Bank has been provided with all the necessary information to credit the payee's account.

If the funds are credited to the account of the payee's bank on a day other than a business day of the bank, it shall be understood for purposes of the first paragraph of this subsection that the payee's bank received the funds for the payee on the first business day thereafter.

As a rule, the user shall announce a cash withdrawal over EUR 2,000.00 to the branch office at least one day in advance or by 11:00 on the same day. The user shall announce a cash withdrawal of more than EUR 2,000.00 via the digital bank at least two (2) days in advance.

The Bank can revert an incorrect credit or debit on the transaction account that was made without the user's order and was caused by a mistake or error by the Bank or its service provider by way of a counter-debit or credit, so that the transaction account balance remains unchanged. The Bank shall notify the user thereof by way of a bank statement delivered in the agreed-on manner. If the user opposes such reconciliation or correction, the Bank will restore the balance prior to the correction immediately after receiving a substantiated complaint.

3.5.11 Restriction on use of funds

If the available account balance is overdrawn (unauthorized negative balance), the Bank will warn the accountholder thereof in writing. The Bank may also restrict the use of selected or all payment instruments for a certain term.

The accountholder hereby acknowledges that the Bank may use all communication channels commonly used by the Bank (direct mail, email, telephone, SMS, digital bank inbox, etc.) to notify and alert them for purposes of performing the Consumer Payment Services Agreement.

In case the accountholder declares personal bankruptcy, the Bank will restrict the use of their account and terminate the regular or extraordinary overdraft facility.

3.6 Payment cards

Each type of payment card referred to in subsection 3.6.1 shall be subject to the provisions of this entire section 3.6. of these T&Cs, unless otherwise provided by respective subsections.

3.6.1 Types of payment cards

The Bank issues the following payment cards:
a) Visa Debit card;
b) Visa charge card;
c) Visa (virtual) Prepaid card.

3.6.2 Cardholder insurance

The holder of a Visa charge card agrees to accept accident insurance in case of accidental death and permanent disability with insurance company Zavarovalnica 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 of Accident Insurance for cardholders are available to cardholders at any Bank branch office.

The holder of a Visa (virtual) Prepaid card agrees to accept in the first year following the issue of the card accident insurance in case of accidental death and permanent disability with insurance company Zavarovalnica 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 of Accident Insurance for cardholders are available to cardholders at any Bank branch office.

3.6.3 Card issuance

The accountholder, authorized user, legal representative, or guardian ("cardholder") is provided with a Visa Debit card/Visa charge card/Visa (virtual) Prepaid card ("card"). The cardholder is provided with a secret, personal PIN known only to them ("PIN"). The Bank will issue only a single charge card to the accountholder. The graphics and design of the card given to the accountholder depends on the selected bundle.

The card is delivered to the cardholder's address, while they can take over the PIN via SMS, via the digital bank, or by mail, if they communicate the preference to the Bank when ordering the card. The Bank will send the card by regular mail and display it in the digital bank. If sent by mail, the PIN is sent by registered mail. The card and the PIN are sent in different parcels posted on different days. If the parcel containing the card is returned to the Bank, the Bank will again notify the cardholder that their card is ready and request of them to claim it. The deadline to claim the card is ninety (90) days of the day when the card was ordered. The Bank will destroy the card after ninety (90) days have passed.

The cardholder shall sign the card by hand immediately after receipt, using a permanent pen. A card is not valid unless signed. A merchant can reject a card payment if the card is not signed. The cardholder shall have full liability for any damage and costs associated with the misuse of an unsigned card.

The virtual prepaid card is not provided to the cardholder in plastic format; the accountholder can see the card data needed for payments in the digital bank.

A Visa Debit card, Visa Prepaid card, and Visa charge card are not available without a contactless payment option.

When a card is ordered, the Bank will share the cardholder's personal data (name, surname, mobile phone number, email) with the external processing centre for purposes of secure online payments, payments at Poins of Sale and ATMs, SMS notifications about payment card-based transactions, for purposes of registering for an using the Flik service, using the mobile wallet, using the Click-to-Pay service, and other payment card-related services.
When a card is ordered, the Bank will also share the cardholder's personal data (name, surname, mobile phone number, email) with the Visa card scheme for purposes of using the Click-to-Pay service with online payments. The Bank will share these data with the Visa card scheme also at any change of data of all pre-existing holders of active payment cards for whom it keeps a mobile phone number and email in its system. The user can request that the card and their personal data be removed from the Click-to-Pay service at any time by calling the Bank's Contact Centre.

3.6.4 Use of card

a) Use of Visa Debit card
The card is non-transferrable and can be used only by the cardholder whose name is shown on the card.

The Visa Debit card is a payment instrument that the user can use:

- At Bank and Post counters: the Visa Debit card is used as a transaction account identification card when using the transaction account and as a bank card. When verifying the identity of a user at a Bank and Post counter, the user is also required to present valid personal ID with a photo.
- At Point of Sale equipped with the Visa or Visa Debit label in Slovenia and abroad: the cardholder initiates a payment order to transfer funds to the credit of the payment account of the Point of Sale holder equipped with the Visa label by:
  - Inserting the card into the POS terminal or tapping it against the terminal and entering their PIN, or
  - By only inserting the card or tapping it against the POS terminal, or
  - By inserting the card or tapping it against the POS terminal and signing the purchase slip with a signature that matches the signature on the card,
  - Having the POS terminal read the magnetic strip and signing the purchase slip with a signature that matches the signature on the card,

  (By request of the cardholder, the Point of Sale needs to issue a purchase slip ("slip") for the payment of goods and services).
  The accountholder shall keep a copy of the slip for their records. The cardholder shall allow the merchant at the Point of Sale to verify the validity of the card and their identity. The accountholder should tap or enter the card or mobile phone (mobile wallets) or enter the PIN only once per transaction. In the opposite case, they should request a failed authorization slip.
- To withdraw cash on ATMs equipped with the Visa label in Slovenia and abroad,
- To deposit cash at OTP banka ATMs;
- For remote purchases (e.g. telesales, mail order), during which the card is not physically present at the Point of Sale, using the method provided by the payee (several possible options):
  - By sharing the card number and expiration date, or
  - By sharing the card number, expiration date, and CVV (three-digit number shown on the back of the card next to the signature field).
- For online purchases, during which the card is not physically present at the Point of Sale, using the method

provided and selected by the payee (several possible options):

- By entering the card number and expiration date, or
- By entering the card number, expiration date, and CVV, or
- By entering the card number, expiration date, and CVV, and confirming the payment in the relevant banking app.

When strong customer authentication is used for remote payment transactions, it includes elements for dynamic linking of the payment transaction with a certain sum and certain payee. The cardholder confirms the online payment by entering their password or using their biometric data in the relevant banking app. Before confirming their identity in the online payment process, the cardholder needs to review the sum of the transaction and name of Point of Sale where they are making the online payment. If the data do not match, they should not confirm the payment and are required to notify the Bank of the event.

The user should employ particular care with remote purchases and shall make sure prior to entering the card data that the Point of Sale and the payment are duly secured. The cardholder is obligated to make purchases only on secure websites and with reliable and verified providers of goods and services. Before making a remote payment, the cardholder shall make sure every time that the seller and its references are credible. The cardholder is obligated to review the online merchant's terms and conditions prior to the payment. Data regarded as security mechanisms (expiration date, card number, CVV) should be entered only after the online purchase has been completed and only the payment needs to be executed.

The cardholder shall ensure that the device they use to make payments without the card is protected against viruses and intrusions. The Bank recommends that the user install quality anti-malware software on the devices that is regularly automatically updated, to activate the firewall on the device, and to regularly update their operating system and other software installed on the device that they use to make online purchases. The cardholder is responsible for the selection, use, and maintenance of the security system used to protect the computer or mobile device that they use for online purchases, and shall have full liability for any damage suffered by the cardholder or the Bank due to malware on the cardholder's computer or mobile device. The user shall protect the access to the device by way of a password or other appropriate protection and shall never leave the device unsupervised.

The cardholder may use the card within the approved spending limits and available account balance. The cardholder can make arrangements to change the spending limit at a Bank branch office or via digital bank. The Bank shall have the right to unilaterally change the sum of spending limits at any time, and shall notify the accountholder thereof by way of a message sent to their digital bank inbox, via SMS, via bank statements sent by mail, or in another manner agreed on with the customer. If the cardholder does not agree with the spending limits, they can make arrangements to change them, unless the Bank changed the limits due to restrictions placed on the accountholder's account.

For card security purposes, the cardholder shall ensure that all procedures at a Point of Sale are carried out in their presence. The cardholder shall keep the card in their possession or under their control at all times while making a payment, shall not lose sight of the card, and shall control the entire payment process at all times. With payments made in online stores, online payments, and mail order and telesales purchases, the cardholder shall comply with all requirements for remote payment confirmation.

The cardholder shall have sole responsibility to collect the cash withdrawn at an ATM. The Bank shall not be liable for any uncollected / forgotten cash.

The Bank shall have no liability if a Point of Sale or ATM does not accept cards or cannot ensure the execution of a payment transaction.

If the cardholder does not ensure sufficient account balance before executing a payment transaction, the Bank shall have the right to reject the authorization of funds to execute the payment transaction.

The cardholder hereby irrevocably authorizes the Bank to debit any sums incurred by using the card in Slovenia or abroad against their transaction account in EUR.

The Bank provides the cardholder with the option to use the Security SMS service to enhance banking security. By using the service, the cardholder, subject to procedure and terms set out in subsection 3.6.10 of these T&Cs, is provided with information on an executed or rejection transaction to their mobile device. If the accountholder receives an SMS about an unknown transaction or a transaction that they did not execute themselves, they shall block the card as soon as possible in accordance with section 3.6.8 of these T&Cs. The cardholder shall regularly monitor their card-based transactions via the digital bank or card statements sent by the Bank. If they notice a transaction that they did not make, they shall notify the Bank thereof as soon as possible.

The cardholder undertakes to handle the card, card data, and other security elements (PIN, OTP) as a good manager to prevent the loss, theft, or misuse of the card. The cardholder shall be liable for the full damage incurred by an unauthorized payment transaction executed due to the cardholder committing fraud or acting wilfully or with gross negligence.

The Bank shall not be liable for damages suffered by the accountholder if a third party gains possession of the card or card data needed to make an online purchase and uses the card to make an online payment, unless the card has been reported stolen or lost in accordance with these T&Cs.

The Bank shall not be liable for the quality of goods and/or services paid for by the cardholder using the card. The cardholder shall not use the card for unlawful purposes, which include purchases of goods and services prohibited by Slovenian law. 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 accountholder party is required to settle their obligations to the Bank irrespective of any dispute at the Point of Sale. The cardholder 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 has been confirmed, it can no longer be cancelled or stopped. A purchase that has been confirmed by the cardholder can only be cancelled at the Point of Sale where it was made.

If the cardholder 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 cardholder's or responsibility to make enquiries on their own regarding the financial instruments or other services which are the subject of the investment decision.

b) Use of Visa charge card

Aside from the manner set forth in this section, the Visa charge card is also used in the manner set forth in point a) of this subsection.

The Bank provides cardholders with an active Instalment Payment Credit Agreement to pay in instalments. The cardholder can opt to pay in 2-24 instalments for every purchase of goods and services between EUR 50.00 and EUR 10,000.00 at all Points of Sale in Slovenia, abroad, or online.

A purchase shall be understood as any purchase of goods and/or services that does not include cash and quasi-cash transactions (using the card to purchase traveller's cheques, cryptocurrencies, foreign cash, lottery tickets, raffle tickets, gaming tokens, credit balances, vouchers that can be exchange for cash, various bets, money transfer, etc.).

Instalment payments are available within the available monthly card spending limit. After making a purchase, the Bank sends an SMS to the cardholder, The cardholder shall text back within one hour and communicate the preferred number of instalments. If the cardholder does not receive an SMS from the Bank, they are obligated to notify the Bank thereof. If the cardholder does not split the transaction into instalments within one hour, they can do so later in the digital bank as well until the end of the billing period by 17:00 (by the 10th day of the month where the billing date is the 18th, by the 20th day of the month where the billing date is the 28th, and by the last day of the month where the billing date is the 8th).

The Bank shall not be responsible if GSM reception is not available to the cardholder on location or when reception is not ensured by the telecommunications provider.

Following the card-based payment, the Bank will reduce the available card spending limit for the total amount of the purchase or payment and any instalment-related fees. Instalments are due for payment every month on the date stipulated by the Instalment Payments Credit Agreement and the cardholder is obligated to settle them at the monthly billing of the cardholder in accordance with the Instalment Payments Credit Agreement and these T&Cs.

The first instalment is due for payment on the first upcoming billing data after the transaction was executed once the transaction has been included on the card statement.

The Bank will release the available card spending limit of the cardholder following every monthly billing date in the amount equal to the paid instalment.

The cardholder will be charged a fee for every instalment paid as part of the by-instalment purchase in accordance with the applicable Fee List. The outstanding and not-yet-due part of the debt is non-interest bearing and the accountholder can repay it early at any time.

The Bank will notify the accountholder on card-related debts by way of a monthly card statement. The accountholder is obligated to regularly monitor the monthly statements. If the accountholder has not been notified by way of a statement about a debt within up to sixty (60) days after making a purchase or withdrawing cash, they are obligated to notify the Bank thereof. The accountholder shall also notify the Bank of any incorrect debits or any other errors.

The Bank will debit card-based debts to the account for which the card was issued. The accountholder undertakes to ensure sufficient account balance to cover the debts and card-related fees by latest until the payment e date. If the accountholder does not ensure sufficient account balance to settle the outstanding debts until the payment due date, the Bank can block the card until sufficient account balance has been ensured. The Bank shall have the right to restrict the use of the card also in case it identifies any difficulties in repaying debts owed to the Bank arising from any title/transaction, and shall notify the accountholder thereof. If the accountholder does not ensure sufficient balance to settle outstanding debts, the Bank will warn the accountholder thereof in writing. The Bank will charge

default interest on any late payments in the amount and in the manner set forth by the applicable Decision on Interest Rates.

The Bank will make the monthly spending limit available on the day when the debt has been repaid in the amount equal to the sums repaid. If debts have not been repaid in full, the Bank will block the card in full after ten (10) days.

c) Use of Visa (virtual) Prepaid card

The use of the Visa Prepaid card is subject to procedures set forth in point a) of this subsection and to additional terms specified below.

The accountholder shall provide funds in the prepaid account via their transaction account and thereby provide balances to be spent with the card and to pay fees and charges for services associated with the prepaid account and card. The prepaid account is intended exclusively for the use of a prepaid card. Prepaid account balances shall be provided by the accountholder by way of money transfers, using the account number and reference shown on the back side of the card or made available to the cardholder via the digital bank in accordance with these T&Cs.

The cardholder can use the card within available spending limits. Cash withdrawals are capped at EUR 350.00 per day and EUR 1,000.00 per month. The Bank shall have the right to unilaterally change the sum of spending limits at any time, and shall notify the accountholder thereof by way of a message sent to their digital bank inbox, via SMS, via bank statements sent by mail, or in another manner agreed on with the customer.

When ordering a card at a Bank or Post counter, the cardholder shall ensure that the card issuance fees will be covered with balances in their account or paid in cash. When ordering a card via the digital bank, the cardholder shall ensure that the card issuance fees will be covered with balances in their account.

The total balance of cash deposits to the prepaid account shall not exceed EUR 2,000.00 per calendar month, and the prepaid account balance is capped at EUR 2,000.00 at any given time. If the limit is exceeded, the funds from the transaction account opened to use the prepaid card will not be transferred to the prepaid account, but will remain on the transaction account linked to the prepaid card.

The cardholder shall ensure sufficient available prepaid account balance to pay sums owed to the Bank arising from fees, charges, exchange rate differences, and any transactions initiated by a merchant that do not require authorization arising from the use of the prepaid card. If the prepaid account balance is too low to pay the obligations, the cardholder irrevocably authorized the Bank to settle sums arising from the use of the card in Slovenia or abroad by a debit to the transaction account linked to the prepaid card in EUR.

3.6.5 Actions of the cardholder to protect a payment card with PIN

The cardholder is obligated to protect those card elements (e.g. PIN) that could enable its unauthorised use. Data shown on the card (card number, expiration date, CVV) are regarded as security credentials of the card and the cardholder shall not share them with anyone other than in case of online payments or remote purchases that require payment.
The cardholder must keep the PIN confidential to prevent misuse. The cardholder must keep the card separate from the PIN and must not lend or give the card to anyone for safekeeping. They must also not write the PIN on a slip or card or otherwise store it with the card. When entering the PIN at an ATM or POS terminal, the holder shall shield the keypad with their hand and thereby ensure that third parties cannot learn the number. The cardholder must memorise the PIN and destroy the PIN notification immediately upon receipt. The cardholder must not disclose the PIN to third parties and must prevent third parties from obtaining unauthorised access to this information and using the card improperly. To make it easier to remember their PIN, the bank allows cardholders to change it at its own 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 cardholder changes the PIN, they shall be responsible for the security of the password they choose. If the cardholder forgets their PIN, they can display their existing PIN in the digital bank or order a new PIN at branches, without having to order a new card.

The cardholder shall not disclose card security credentials by phone, 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. The cardholder 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 cardholder 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, including payment card numbers, user names and passwords. This information must be kept secure by the cardholder and must not be disclosed in such way. In addition, the cardholder must not allow remote access to their computer or mobile device to any unauthorised person.

The cardholder shall use the card with care, preventing to the maximum extent possible its misuse, loss and unauthorised confiscation and thus preventing material loss from being incurred by themselves and the Bank. The cardholder must not leave the card unattended (e.g. in the car, office, public area, hotel room, pub, etc.). The holder can temporarily block and unblock payment cards at any time via the digital bank.

Failure to comply with the obligations set out in section 3.6 is considered gross negligence on the part of the cardholder. The cardholder shall be fully liable for any consequences of PIN misuse resulting from the failure to comply with the practices described in this section.

The cardholder 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 otpbanka.si/varno-poslovanje-s-placilnimi-karticami, where the Bank provides guidance on the safe use of cards and warns about various online fraud attempts and how to identify them.

3.6.6 Fees

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

If the holder withdraws its application between the time the card is ordered and prior to the card being issued, they must pay the costs related to issuing the card.

3.6.7 Validity and termination of the right to use the card

a) Visa debit card

The card is valid until the last day of the month indicated on the card. The Bank will renew the membership of holders who operate in accordance with these T&Cs without a new application. In the event of termination of the agreement or when the Bank is notified of the death of the holder, all cards of the holder and the authorised userss cease to be valid, regardless of the validity period stated on the card.

The card is the property of the Bank, therefore the cardholder is required to return the card if so requested by the Bank. The cardholder 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 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 increased risk that the user will not be able to meet their payment obligations and the use of the card is associated with a loan approved to the user.

The Bank will notify the cardholder of the card blocking and the reasons for it in the usual manner for the Bank, 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 will enable the card to be used again when the reasons for the blocking cease to exist or when it replaces the blocked card with a new one.

The Bank shall have the right to temporarily prevent the cardholder (except for the holder of a payment account with basic features) from using their card by blocking it if the cardholder does not comply with the Bank's request to deliver missing/incomplete documentation that the Bank is required to collect from the client based on the law and does not provide the documentation within the deadline the Bank sets in its request. The Bank will send the request to the cardholder via the communication channel used by the cardholder. In the case of an authorised user, the Bank also forwards the request to the account holder. The Bank will reactivate the cardholder's card once the cardholder has provided the Bank with the requested documentation.

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

The account holder agrees to settle all obligations to the Bank arising from the use of the card that the Bank receives, even after the transaction account is closed and the Bank was not aware of them at the time the account was closed.

The cardholder shall regularly monitor all notifications concerning payment security.

b) Visa charge card and (virtual) Visa prepaid card

The provisions of point a) of this subsection shall apply mutatis mutandis to the validity and right to use of charge cards and (virtual) prepaid cards, as well as additional provisions as specified below.

If the cardholder does not wish to renew their membership, they must cancel their membership in person at a bank branch or in writing by registered mail addressed to the bank branch that approved the card, at least two (2) months before the card expires or before the annual membership fee is accounted for, otherwise the Bank will recharge the annual membership fee in accordance with the Fee List. In this case, the holder is obliged to return the card to the Bank. The Bank has the right not to renew the cardholder's membership if the cardholder has not used the card for 12 months, of which the Bank shall notify the cardholder by sending a message to the digital bank inbox, by SMS message, by mail with statements or independently, or in another manner agreed upon with the customer. In this

case, the agreement shall cease to be valid and the holder shall be obliged to act as directed in the second paragraph of point a) of this subsection.

The automatically renewed card (with the exception of a virtual prepaid card) is sent by the Bank to the cardholder by mail to their last known address. After the card's validity expires, the holder is obliged to destroy the old card so that the card number can no longer be recognised. The details of the renewed virtual prepaid card can be seen by the holder in their digital bank.

If the use of the card is prohibited, the holder must immediately provide coverage for all liabilities related to card transactions.

In the event of a ban on the use of the card, the cardholder is obliged to immediately stop using the card and return it to the Bank within seven (7) days of receiving the ban and immediately provide coverage for all liabilities related to card transactions. Otherwise, the Bank will charge the cardholder all costs incurred after the day the card should have been returned, in accordance with the Fee List.

The Bank shall notify the point of sale network about the prohibition of card use An employee at a point of sale may retain the card based on the Bank's notification. The cardholder shall not use a card that has been cancelled and shall destroy it (cut it through the middle) and return it to the Bank.

In the event of a change in card type, the old card will be cancelled within one month of ordering the card. Upon cancellation of the card, the account holder will receive a refund of the proportional share of the membership fee (if any) to the card account.

3.6.8 Lost, stolen or misused card

The cardholder shall immediately notify, in person or in writing, 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. Phone numbers are published on the Bank's website. The phone 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.

In the event of theft or misuse or suspected theft or misuse, the cardholder 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 cardholder is obliged to provide the Bank with all the necessary information about the circumstances related to the loss, theft or misuse of the card. The cardholder must confirm in writing a phone report of loss or theft of the card within seven (7) days.

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

If the cardholder 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.

3.6.9 Incoming card payments

The cardholder 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.

If the cardholder knowingly uses the card to receive incoming payments, the Bank may notify the competent institutions in this regard. The Bank shall not be liable for these actions of the cardholder. If the cardholder 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 transaction account on the maturity date.

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

3.6.10.1 Basic information

The SMS transaction alert service for card transactions is a method of providing information to holders of payment cards by way of text messages to their mobile phones (of Slovenian operators). The holder receives an SMS message about the completed transaction when authorisation is completed. The transaction amount may deviate from the previously authorised amount in certain cases, especially in restaurants, petrol stations, hotels and car rental services.

The service can only be used by the holder of the payment card.

3.6.10.2 Terms and conditions and approval of use of the service

The account holder may order the SMS messaging service for themselves and their authorised users. The authorised users of the 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 account holder.

When opening a bundled account, the Bank, together with the user, determines the payment cards for which the user will receive SMS messages about payment card transactions.

3.6.10.3 Cancelling a service order

The service user may cancel the SMS transaction alert service for card transactions by way of a written cancellation notice submitted at a bank branch office.

If the Bank finds that the user breached the provisions of these T&Cs, the provisions of the transaction account agreement, or abused the right of service subscription, or caused the Bank damage in any other way, it reserves the right to cancel the service.

3.6.10.4 Fees

The Bank shall charge the user a fee and costs for the SMS transaction alert service in accordance with the Fee List applicable at the time.

3.6.10.5 Rights and obligations of the users of SMS transaction alert service for card transactions

The service user must provide the Bank with a correct and valid mobile phone number and is responsible for the correctness of the data provided when opening a transaction account for the service of SMS transaction alert service for transactions with the Bank's payment cards. 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 phone number and shall not be liable if the mobile phone number is incorrect or invalid. The user 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 does not assume any liability for damage caused by theft or loss of a mobile phone or SIM card, for undelivered or late-delivered SMS messages from the mobile operator, or other irregularities not caused by the Bank.

The user shall be solely responsible for the security and confidentiality of data stored in the mobile phone.

3.7 Digital bank (online and mobile banking)

3.7.1 Basic information

The Bank@Net online bank and the mBank@Net mobile bank ("digital bank") provide the user with secure and fast access to banking services or access to bank transactions. The Bank@Net online bank is accessible via a browser, while the mBank@Net mobile bank is a mobile application intended for banking services on a mobile device on which the application can be installed.

The user is simultaneously a user of the Bank@Net online bank and the mBank@Net mobile bank. The Bank enables the user to use the digital bank by creating a user account. The user account is accessible to the user by using the assigned personal security credentials, and the user thereby gains secure access to their bank accounts and banking services, including managing accounts and contracts, executing and processing payments, transferring funds, concluding products, and other services offered by the digital bank.

When subscribing to use the digital bank, the user receives an SMS token security credential, which consists of:

- User name;
- The first assigned password (when subscribing in a branch; this password must be reset immediately) or a personal password (when activating online; this password is set by the user).

When using mobile banking for the first time, the user sets a PIN and thereby activates the mobile token security credential. After activation, the user has the option to set the use of biometrics.

The user can make payments and use other services 24/7. Confirmation with personal security credentials is considered to be the conclusion of a contract or the performance of a remote service. In the event of concluding a product or service through the digital bank, the Bank charges fees in accordance with the applicable Fee List. There are no additional costs when concluding a product or service through the digital bank.

Currency conversions at the Exchange Office are performed every business day, Monday through Friday, from 7:00 to 18:00. Any conversion requests confirmed outside of these hours will be processed the next business day. The conversion rate displayed upon confirmation of the request is for informational purposes only. The exchange rate valid at the time of conversion will be used for conversion. The maximum total amount of all conversions in one day is EUR 10,000 or the equivalent in another foreign currency.

3.7.2 Data processing and analysis

The user confirms that they are aware of and agree that the Bank may monitor the use of the digital bank and its services for statistical purposes and to prevent abuse, therefore the digital bank may:

- Record critical errors (application, browser and operating system version);
- Process and analyse data about user activities in applications;
- Use data in anonymous form for statistical processing.

More detailed information on privacy protection and data collection is provided in the Privacy Statements published on the Bank's website Price lists and Tterms and conditions | OTP in the documents mBank@Net - Privacy Statement and Bank@Net - Privacy Statement.

3.7.3 Authorisation to use and access the user account

Only a person who has an open transaction or prepaid account with the Bank can be a digital bank user. The Bank does not allow the use of digital banking on the account of a holder who is placed under guardianship.

Upon authorisation to use the digital bank, the Bank assigns personal security credential to the user at a branch or remotely for secure login to the user account and secure provision and performance of services.

The user must ensure access to the Internet or enable data connections on a computer or mobile device ("device") and appropriate hardware that meets the minimum technical requirements listed on the Bank's websiteBank@Net help services | OTP.

The user undertakes to bear all data transfer costs of the selected telecommunications service provider incurred when using the application. The instructions for using the application are published on the Bank's website Bank@Net help services | OTP. Information regarding the safe use of the application is available on the Bank's website Online banking security | OTP.

3.7.3.1 Ways of accessing

When logging into the digital bank, the user enters personal security credentials in accordance with the description on the Bank's website Bank@Net help login | OTP.

To access the functionality, the digital bank user must log in to their user account.

The user can log in to the online bank in the following ways:
- With an SMS token – the user enters their user name and personal password each time they log in and enters a one-time SMS token;
- By selecting the "Remember me" option, which saves the user name locally on the personal computer and only requires entering the password when using the online bank (IMPORTANT: the user may not use the "Remember me" option on a foreign or public computer);
- with a mobile token – the user enters a user name and a one-time password that they create in the mobile bank.

The user can log in to the mobile bank mBank@Net in the following ways:
- With an SMS token – the user enters their user name and personal password each time they log in and enters a one-time SMS token. In versions of the mobile bank that allow mobile token activation and the mobile token is activated on the device, this login method is not possible;
- With mPassword – the user connects the device to their user account. In versions of the mobile bank that allow mobile token activation, setting an mPassword is not possible;
- With a mobile token – by entering the PIN set;
- With biometric login (fingerprint or facial recognition) – enabled only if an mPassword is set on the device in the mobile bank or a mobile token is activated. IMPORTANT: Biometric login is intended exclusively for the device owner. The user is responsible for ensuring that only their biometric data is stored in the device. If other people's data is stored on the device, these people can access the application and perform activities in the digital bank.

3.7.3.2 Methods of confirming payments and other requests

Confirmation of payments and other requests in the online bank is possible in the following ways:
- With an SMS token – the user enters a one-time SMS token;
- With a mobile token – the user confirms the request in the mobile bank (enters a PIN or uses biometrics).

Confirmation of payments and other requests in the mobile bank is possible in the following ways:
- With an SMS token – the user enters a one-time SMS token;
  With a mobile token – the user enters a PIN or uses biometrics.

3.7.4 User rights and obligations

The user undertakes to carefully protect their personal security credentials as a good manager, preventing loss, theft or misuse, and not to communicate or hand them over to any person. The user undertakes not to entrust his/her user name, password and PIN for access to the digital bank, as well as the received one-time passwords or SMS tokens, to anyone and to carefully protect them in a way that prevents a third party from becoming aware of them.

By using the digital bank, the user agrees to receive SMS messages to their mobile number containing one-time passwords (SMS token) for login and confirmation of requests or other notifications from the Bank that are related to the use of the digital bank and mandatory for using the digital bank.

The user shall protect the access to the device by way of a password or other appropriate protection and shall never leave the device unsupervised. The user undertakes not to enable remote access to their computer or mobile device to any unauthorised person.

The user undertakes to store only their biometric data on their device. If a user stores biometric data of other people on their device, there may be a possibility of misuse, such as login and transactions by an unauthorised person.

In the event of loss or theft of the mobile device, the user undertakes to immediately unbind it via the Bank@Net online bank in accordance with the information for using the digital bank, available on the Bank's website otpbanka.si/bnks. The user must immediately report any loss/theft of the device or security credentials to the Bank. The user shall inform the Bank's contact centre. The contacts are published on the Bank's website.

The use of the digital bank will be blocked after receipt of the report. The user is solely responsible for any damage that may arise from any misuse resulting from failure to follow the instructions and regulations.

The user will use the digital bank in accordance with the information for using the digital bank available on the Bank's website. Bank@Net help services | OTP. The user shall be solely responsible for the security and confidentiality of data stored on the device. The Bank does not assume any responsibility for any misuse of data stored on the device.

The Bank does not assume any responsibility for any damage caused by the user’s improper and careless handling of the application or device.

The user undertakes to protect the device through which they will access the digital bank from viruses and intrusions, and to regularly monitor notifications from the Google Play, App Store and Huawei App Gallery mobile stores and download new versions of the mBank@Net application, thus enabling access to all new features.

The mBank@Net application is updated automatically if the user has automatic application updates turned on. If the user does not have automatic updates turned on, they must update the application manually to ensure smooth transactions with the appropriate version of the mobile bank. The Bank is not liable for any damage caused by an outdated mobile application. The Bank reserves the right to disable the use of mobile banking if the user does not have a properly updated mobile application.

The user must regularly monitor their transactions. If they notice a transaction that they did not make, they shall notify the Bank thereof as soon as possible.

The account holder can set the value of the daily limit for account transactions via the digital bank or the limit for instant payment in the digital bank, a bank branch or through the contact centre. The authorised user can change the daily limit for account transactions via the digital bank up to a certain value themselves at a bank branch or with the help of the contact centre; any additional changes can only be made in the presence of the account holder.

The user must always carefully check the content of the received SMS message from the Bank with a one-time password or SMS token before entering it into the device. If the user receives an SMS token to confirm a transaction that is unknown to them and that they did not carry out themselves, they must immediately notify the Bank, block the digital bank and bank cards.

The user undertakes to verify the correctness of all payment data before further use of the payment created by the application from the received link by reading the QR code or from an imported document containing a QR code. Any further use of the payment constitutes agreement with the content by the user.

The user shall be liable for the full damage incurred by an unauthorised payment transaction executed due to the user committing fraud or acting wilfully or with gross negligence.

The user must immediately notify the Bank of any identified irregularities or unusual functioning of the digital bank. In the event of misuse or suspected misuse of the digital bank, and of any unauthorised use or suspected unauthorised use of the digital bank, the user must immediately notify the Bank's contact centre and submit a request for blocking. The contacts are published on the Bank's website.

The user must pay attention to any received electronic or SMS/MMS messages with links to websites. They must not enter personal or account information, card details, or security credentials on these websites. The user 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, payment card numbers, user names and passwords. This information must be kept secure by the user and must not be disclosed. Failure to comply with the security mechanisms and the user's obligations set out in this section is considered gross negligence on the part of the user.

The user must regularly monitor and review Bank's notifications and account transactions.

The user agrees to receive commercial messages and contacts from the Bank to improve services. In versions of the mobile bank that do not yet enable activation of the mobile token, setting the mPassword is a prerequisite for receiving push messages confirming the payer's identity when making an online payment.

The user shall be fully liable for any consequences of security credentials misuse resulting from the failure to comply with the practices described in this section. The user shall also comply with any other instructions, warnings or advice of the Bank relating to the use of the digital bank. Information on the safe use of the digital bank is published on the Bank's website Online banking security | OTP, where the Bank provides guidance on the safe online banking and warns about various online fraud attempts and how to identify them.

3.7.5 Bank's rights and obligations

The Bank keeps records of the use of services in accordance with applicable legislation. When the digital bank is used, the Bank will record the use of services in a computerised manner and will ensure the appropriate storage of these records in accordance with existing legislation.

The Bank is not responsible for any disruptions in telecommunications networks or for any errors in data transmission over telecommunications networks. The Bank is not liable for any damage incurred as a result of improper user behaviour or incorrect data entry by the application user.

All bank account statements, card transaction statements and other bank notifications (messages) in the Inbox, as well as all user requests (e.g. payments made, orders or other requests) shall be available to the user via the digital bank for 24 months. After 24 months, the Bank archives the aforementioned documentation and it is only accessible upon request by the user. The user must archive the documentation they want to keep outside the digital bank after it is no longer available in the digital bank Inbox.

The Bank does not assume liability for any damage that may arise from any misuse as a result of failure to follow the instructions related to the incorrect use of biometric data or data related to biometric data, as specified in these T&Cs. The Bank does not assume liability for the accuracy of the data generated by the application (scanning the universal payment order code, importing a document with a QR code when paying a universal payment order or received e-Invoices, or received external links for creating payments), nor for the accuracy of the locations of ATMs and branches.

The Bank does not guarantee a flawless operation of the application's functionalities which depend on individual hardware components on/in an individual device (e.g. scanning a QR code for payment, updating an identity document, etc.).

The Bank may disable or temporarily block the user's access to the digital bank at any time if:

- The user is using an outdated version of the mobile bank, until the user updates the application to the appropriate version, either voluntarily or upon the Bank's request;
- The user loses or has their device stolen;
- There is any suspicion of unauthorised access;
- The user has a VPN service turned on or is connected to a virtual private network, in which case access to the digital bank is not enabled;
- There are objectively justified reasons associated with the security of the digital bank (e.g. reasons to suspect that the digital bank could be misused or data stolen via the digital bank, etc.);
- The user violates these T&Cs.

The Bank shall notify the user of the blocking of the access to the digital bank and the reasons for it in the usual manner for the Bank, if possible before the access to the digital bank is blocked, and no later than after blocking, except where such notification is contrary to objectively justified security measures. The Bank shall enable access to the digital bank again when the reasons for the blockage cease to exist.

For a Bank@Net and mBank@Net user who is also a user of eBank@Net com, Bank@Net com and mBank@Net com or Poslovni Bank@Net, the Bank may at any time disable the use of any of the listed digital channels in full functionality or terminate the use of any of the listed digital channels with immediate effect.

The Bank shall have the right to temporarily prevent the user (except for the holder of a payment account with basic features) from accessing the digital bank if the user does not comply with the Bank's request to deliver missing/incomplete documentation that the Bank is required to collect from the client based on the law and does not provide the documentation within the deadline the Bank sets in its request. The Bank shall forward the request to the user via the communication channel used by the user. In the case of an authorised user, the Bank shall also forward the request to the account holder. The Bank shall enable the user to regain access to the digital bank once the user has submitted the required documentation to the Bank.

The Bank may also cease providing the service if the user fails to fulfil their obligations.

The Bank shall provide the user with all services accessible through the digital bank in accordance with these T&Cs.

3.7.6 Risk management and prevention of misuse

The user confirms the use of measures by the Bank to manage risks and prevent misuse, including tools for the detection and prevention of financial crime, in accordance with relevant laws and regulations. These measures may include assessing the security of the user's device for possible malware infections, investigating and reporting to prevent financial crime, and managing user risks in accordance with laws and regulations applicable to the Bank.

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 device from which they access the digital bank and shall be fully liable for any damage incurred by them or the Bank as a result of malicious software on their device.

The Bank is not liable for any damage suffered by the user if a third party becomes aware of the user name and password and the security credentials required for login and unauthorisedly accesses the user's digital bank and performs transactions. In case of suspicion of unauthorised use, the Bank may disable the use of the digital bank.

Information on the safe use of the digital bank and minimum requirements for suitable operating systems are available on the Bank's website Online banking security | OTP, where the Bank provides guidance on the safe online banking and warns about various online fraud attempts and how to identify them.

The user shall also comply with any other instructions, warnings or advice of the Bank relating to the use of the digital bank.

3.7.7 Cancelling the use of the digital bank

The use of the digital bank ceases with the closure of the transaction account. The user can cancel the use of the digital bank in writing by submitting a request to a bank branch, with a notice period of seven (7) business days, counted from the day the Bank receives the written cancellation.

The user must settle all due liabilities to the Bank that arose when using the digital bank by the end of the notice period. The user authorises the Bank to settle all overdue liabilities by debiting the user's transaction account in the event of non-fulfilment of obligations, but if this is not possible, the user undertakes to settle all overdue liabilities himself/herself.

The user must, in accordance with these T&Cs, ensure that they do not have any payment orders pending on the date of expiry of the notice period. If the user does not arrange the status of pending payments with an execution date after the cancellation of the digital bank before cancellation, these payments shall be executed on the selected date.

3.7.8 e-Invoice / e-Document service

The recipient of an e-invoice must have a transaction account with the Bank through which they will provide services in the e-Invoice Exchange System.

The recipient of an e-document must have a transaction account registered in the digital bank through which the e-invoice service will be provided, or must have a transaction account registered in the digital bank of the authorised user.

1. The recipient of e-invoice:
    - Is obliged to complete an e-subscription for receiving e-invoices via the digital bank or subscribe to receiving e-invoices with the e-invoice issuer;
    - Is obliged to accept e-invoices from the issuer for which they have completed an e-subscription or subscription with the e-invoice issuer;
    - Has the right to receive and view e-invoices for which they have subscribed via the digital bank;
    - Can stop using the e-invoice service and unsubscribe from the service via the digital bank;
    - Can stop receiving e-invoices from an individual issuer and e-unsubscribe from receiving e-invoices via the digital bank or unsubscribe from receiving e-invoices from the issuer of e-invoices;
    - Is obliged to inform the issuer of the e-document of any change related to the receipt of e-invoices and is obliged to ensure that the method of receiving e-invoices from the issuer of e-invoices is changed upon:
        - termination of the transaction account through which the e-invoice service is provided at the Bank;
        - unsubscription from the digital banking service by the user or by the Bank;
    - shall ensure the archiving of e-documents.

2. Authorisations of a digital bank user when using the e-invoice service on an individual transaction account:
    - The transaction account holder can receive and view e-invoices, perform e-subscriptions for or e-unsubscriptions from receiving e-invoices and make e-invoice payments via the digital bank on an individual transaction account. The authorisations of the transaction account holder do not apply if the user has an assigned legal representative or guardian;
    - A person authorised by the recipient of e-invoices to dispose of funds in the transaction account of the recipient of e-invoices ("authorised user") may receive and view e-invoices and make payments for e-invoices through the digital bank on the transaction account for which they are authorised, but they cannot perform e-subscription for

or e-unsubscription from receiving e-invoices in their own name or on behalf of the personal account holder. The authorised user is obliged to inform the recipient of e-invoices about any changes related to the receipt of e-invoices;
- The legal representative/guardian of the transaction account user can receive and view e-invoices via the digital bank, perform e-subscriptions for or e-unsubscriptions from receiving e-invoices, and make e-document payments.

3. The Bank, acting as the recipient's bank, is obliged to:
- Send a correctly received e-invoice and make it available to the recipient of e-invoices via the digital bank;
- Send feedback to the issuer's bank that the e-invoice has been sent to the recipient of e-invoices or that the e-invoice cannot be sent to them;
- Enable the recipient of e-invoices to e-subscribe for or e-unsubscribe from the receipt of e-documents via a digital channel and provide the recipient of e-invoices with the possibility of providing feedback on the sent e-subscription for or e-unsubscription from the receipt of e-invoices;
- Enable the recipient of e-documents to unsubscribe from the e-invoice service;
- Ensure the exchange of correctly created e-invoices, e-subscriptions for and e-unsubscriptions from the receipt of e-invoices and feedback in accordance with the applicable payment service schedule;
- Reject an e-document if:
  - the e-invoice or attachments are not in accordance with the Manual for e-invoice exchange published on the website of the Bank Association of Slovenia www.zbs-giz.si/;
  - the recipient of the e-invoice does not have an account open with the Bank or the e-invoice recipient's account is not registered through the digital bank;
  - the bank of the recipient of the e-invoice is not included in the e-Invoice Exchange System.

The Bank does not provide e-invoice storage services for e-invoice recipients.

3.8 e-Notifications service

3.8.1 Basic information

The e-Notifications service is intended for users who are over 15 years old, do not use the digital bank, and have at least one active product with the Bank. It enables the user to access, through e-mail or SMS message, the e-Notifications portal and all notifications for:
- Personal account;
- Card transactions;
- Loans;
- Deposits and savings;
- Collateral;
- Other.

On the e-Notifications portal, the Bank enables the user to review e-Notifications for a period of 24 months.

3.8.2 Approval of the use of the e-Notifications service

A person who has at least one product with the Bank and whose mobile phone number and email address are available to the Bank can apply to use the e-Notifications service. The user can subscribe to the e-Notifications service at a bank branch.

If the user already uses the digital bank, subscribing to the e-Notifications service will terminate access to the digital bank.

The Bank decides on the subscription to the e-Notifications service. The Bank reserves the right to refuse application for subscription without explanation.

3.8.3 Using the e-Notifications portal

To use the e-Notifications portal, the user must have access to the Internet and suitable computer equipment. Minimum technical requirements and instructions for using the e-Notifications portal are published on the Bank's website Bank@Net help services | OTP.

Information regarding the safe use is available on the Bank's website Online banking security | OTP.

3.8.4 Accessing the service

The user can access the e-Notifications portal via a link received by email or SMS message. To log in, the user must enter a security code and an SMS token that they receive on their mobile number.

3.8.5 User rights and obligations when using the e-Notifications service

The user undertakes to immediately notify the Bank of any loss or theft of the mobile device. The user shall inform the Bank's contact centre by phone. The phone number of the contact centre is published on the Bank's website. The use of the e-Notifications service shall be blocked after receipt of the report.

In the event of a change in mobile number, the user must visit a bank branch, while changing the email address can be done by visiting a branch or through the contact centre.

3.8.6 Cancelling the e-Notifications service

The user can cancel the e-Notifications service in writing by submitting a request to a bank branch, with a notice period of seven (7) business days, counted from the day the Bank receives the written cancellation.

The use of the e-Notifications service is automatically terminated if the user subscribes to the digital bank.

3.9 Using the mobile wallet of the Bank and other providers

3.9.1 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 cardholder decides independently whether to accept the terms and conditions of the mobile wallet provided by a particular mobile wallet provider. The cardholder 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 cardholder accepts before starting to use the mobile wallet.

3.9.2 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.

3.9.3 Adding a payment card to the mobile wallet

The cardholder 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 cardholder must reload the new card into the mobile wallet. The holder can load the card in multiple mobile wallets or on multiple devices. The cardholder 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.

Mobile wallet providers may have certain restrictions on the use of the mobile wallet, such as an age limit or a limit on the number of cards that can be added to the mobile wallet, or specific security checks and technical requirements. The cardholder must therefore check whether they meet the requirements of the individual mobile wallet.

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 cardholder 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.

3.9.4 Provision of payment services

The user can use the mobile wallet to place a payment order to transfer funds to 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.

The user can order a payment transaction at a POS terminal, or withdraw and deposit cash, or check the balance at a contactless ATM in the following way:

- At the point of sale and contactless ATM:
  - in the case of a payment card, the user brings their 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;

- Sending money and sending a request to receive money:
  - Within the application, the user selects or manually enters the contact information of the recipient of the payment or payment request via the Flik payment instrument.

The provisions of section 3.5 of these T&Cs apply to the execution of a payment transaction.

A card that is invalid or blocked cannot be used. The Bank can also block the card in case of suspected misuse.
The mobile wallet provider may also restrict the use of a digitised card in the event of violations of its general terms and conditions or its rules in the system for monitoring and preventing misuse.

3.9.5 FLIK

The user can perform the following services through Flik:

- Sending instant payments to a recipient who has a defined contact in the Flik phonebook;
- Sending payment requests to a recipient who has a defined contact in the Flik phonebook;
- Receiving instant payments if the user has at least one contact defined in the Flik phonebook;
- Receiving payment requests if the user has at least one contact defined in the Flik phonebook;
- Checking the balance and status of transactions made with Flik;
- Managing one's contacts in the Flik phonebook;
- Paying at physical and online points of sale;
- Managing the allowed daily transaction amount;
- Managing one’s mobile devices;
- Changing one’s password and setting up one’s fingerprint or facial recognition;
- Receiving notifications;
- Changing language settings;
- Viewing and changing other settings of the Flik mobile application.

A user may submit a maximum of ten (10) payment requests per day.
The user can make a one-time payment via the NFC interface without logging into the mobile wallet. When making Flik payments, the limit for instant payments on the transaction account is taken into account and if it is exceeded, the Bank rejects the order.

The mobile wallet user shall bear the entire loss of the amount of an unauthorised payment transaction and the associated fees and interest if the execution of the unauthorised payment transaction:

- Results from fraud and/or scam by the mobile wallet user or if the mobile wallet user intentionally or through gross negligence failed to fulfil their obligations regarding measures to protect the mobile device in accordance with these T&Cs and the personal password on the mobile device in accordance with these T&Cs;
- Results from a violation of these T&Cs by the mobile wallet user.

The mobile wallet user shall bear the loss of the amount of an unauthorised payment transaction and the associated fees and interest of up to 50.00 EUR if the execution of the unauthorised payment transaction results from the use of:

- A stolen or lost mobile device (such as password misuse, unauthorised registration, etc.);
- A mobile device that has been misused if the mobile wallet user has not secured the personal security credentials of the payment instrument in accordance with these T&Cs.

If the user is entitled to a refund of the payment transaction amount, the Bank shall transfer the payment transaction amount to the user's account within thirty (30) days at the latest, unless a longer period is required due to the circumstances of the individual case (of which the user will be notified in an agreed manner).

3.9.6 Financial Flik complaints in relation to paying for purchases at the point of sale

The mobile wallet user as the payer of the purchase and the merchant as the recipient of payment for the purchase are entitled to file a financial Flik complaint (“complaint”) against an individual transaction with respect to Flik transactions carried out at the merchant's points of sale (“transaction”), in the cases listed below when:

a. The transaction was not completed, with the user receiving information that the transaction was successfully completed, and the merchant receiving information that the transaction was not completed;
b. The user does not recognise the transaction (when reviewing the account transactions, the user does not recognise the point of sale where the transaction was supposedly made);
c. The user was charged multiple times for a single purchase or the user was informed that the transaction was unsuccessful and paid for the purchase with another payment method;
d. The user noticed after the transaction that the transaction amount was not the same as the price amount on the invoice issued to them by the merchant;
e. The user did not make the transaction and believes it is abuse.

If the complaint regarding an individual purchase/payment made via the mobile wallet is not related to the reasons from the previous point, the mobile wallet user is obliged to immediately and without delay notify the Bank of the unauthorised and/or unexecuted payment transaction upon discovering that such payment transactions have occurred, but no later than thirteen (13) months after the debit date. If the Bank is responsible for the failure to execute or incorrect execution of a payment transaction or the execution of an unauthorised payment transaction, it must immediately refund to the mobile wallet user the amount of the unauthorised payment transaction and all charged fees and interest to which they are entitled, to the mobile wallet user's personal account. The Bank shall be relieved from liability to refund the sums of unauthorised payment transactions:

- If the execution of unauthorised payment transactions is the result of extraordinary and unforeseeable circumstances that it cannot influence or does not manage to influence despite all its efforts;
- If the obligation to execute a payment transaction results from other regulations binding for the Bank;
- If the unauthorised payment transaction was caused by the mobile wallet user committing fraud or because the user failed to meet their obligations in relation to the payment instrument wilfully or due to gross negligence;
- In the part covered by the mobile wallet user, if the execution of an unauthorised payment transaction is the result of using a stolen or lost payment instrument or a payment instrument that was misused (if the mobile wallet user failed to protect the personal security credentials of the payment instrument);
- If the mobile wallet user fails to immediately and without delay notify the Bank of an unauthorised and/or unexecuted payment transaction upon becoming aware that such payment transactions have occurred.

The mobile wallet user undertakes to primarily resolve complaints regarding non-receipt of goods/services, inadequate, non-functioning or defective goods/services, cancelled goods/services and counterfeit goods/services themselves with the merchant or point of sale.

In accordance with the interbank complaint resolution procedure within the Flik scheme, the Bank accepts and examines complaints from users and merchants. The user must submit to the Bank an explanation of the complaint and all evidence of the transaction to which the complaint relates. The evidence is considered to be in particular (but is not limited to) the following: a screenshot of the mobile wallet on the user's smart device, a merchant's invoice for the goods displayed or the service provided, a statement of business transactions on the customer's transaction account, etc.

If a well-founded financial complaint is filed, the disputed transactions will be credited to the mobile wallet user's personal account. A complaint is considered to be well-founded if the Bank has received from the user all appropriate evidence that is necessary to initiate the complaint procedure. In the event of a negatively resolved financial complaint, when the recipient of the payment (merchant, etc.) has proven a justified rejection of the complaint within the prescribed period, the mobile wallet user expressly and irrevocably allows the Bank, after the financial complaint procedure has been completed, to re-debit the personal account for the amount that was credited to them upon successfully filing a financial complaint without the specific explicit consent of the mobile wallet user in each case.

The mobile wallet user shall be notified by the Bank about the status of the filed financial complaint within eight (8) business days of receiving the complaint.

3.9.7 User obligations and mobile wallet security

The mobile wallet user undertakes to:

- Carefully protect the mobile device and keep its security credentials, handle it like a good manager in order to prevent theft, loss or misuse, and not to make the mobile device available to third parties. The user shall be responsible for any damage caused by third parties using their mobile device;
- Secure access to their mobile device with security credentials 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 wallet is installed;
- Ensure that the device on which the mobile wallet is installed is protected from viruses and intrusions. 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 programs onto the mobile device that could interfere with or harm the mobile wallet. If the user causes damage out of negligence, they shall be fully liable for it;
- Regularly monitor the notices in the Google Play or App Store mobile store, 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 application in accordance with the provisions of these T&Cs and 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 application or mobile device.

3.9.8 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 mobile wallet is installed, with the aim of deregistering the mobile wallet, to the phone number of the Bank's contact centre, or notify the Bank in person or in writing. The phone number of the Bank's contact centre is 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 card. If the user loses their physical card or the card is stolen, the card registered in the mobile wallet also ceases to function after its blocking.

3.9.9 Obligations of the Bank

The Bank undertakes to:
- Perform its obligations in accordance with these T&Cs;
- Execute the orders for the execution of a payment transaction made through Flik in accordance with these T&Cs and applicable legislation;
- Notify the user of any changes or amendments to these T&Cs and the Consumer Banking Fee List, and the content of the aforementioned documents will be published on the website and in the Bank's branches;
- Inform the user about any novelties in relation to the mobile wallet, but not also in relation to the mobile wallets of other providers;
- Ensure that the Bank's mobile wallet is accessible at all times, although it is possible that the quality of the service or access to it may sometimes be difficult or impossible due to reasons beyond its control. The operation of the system may also be disrupted or interrupted because the system that supports the operation of the Bank's mobile wallet must be periodically maintained, upgraded, and the like.

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.

3.9.10 Fees

The Bank will charge the mobile wallet user costs and fees in accordance with the applicable Consumer Banking Fee List. The use of mobile application may result in mobile data charges for the user.
The mobile wallet provider may charge its own fees for using the mobile wallet.

3.10 Additional services related to transaction accounts

3.10.1 Notification on account activity

Notification on account activity is a service that sends SMS messages and/or emails when changes occur in a transaction account. When activating the notification service, the user selects the change they want to be notified about. They can choose between being notified about:
- the balance on the transaction account;
- the inflows to the transaction account;
- the outflows from the transaction account;
- the expiry of deposit;
- the expiry of transaction account overdraft;
- successfully processed and/or declined payments;
- SEPA direct debits received.

In the case of notification of the balance on the transaction account, the holder has the option to choose any notification date (e.g. day of the week or month or daily notification) and notification time. The user can include all transaction accounts of which they are the holder and all transaction accounts for which they are authorised in the notification on account activity.

The service is charged in accordance with the applicable Fee List.

3.10.2 SEPA direct debit ("SEPA DD") for the payer according to the basic scheme

3.10.2.1 Mandate

The payer and the payee agree on settling of the payer's obligations by means of SEPA DD whereby the payer issues a 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 payer's 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 thirty-six (36) months after giving the mandate.

3.10.2.2 Executing SEPA DD payment orders

The payer's bank shall execute a SEPA DD payment transaction on the execution date if the payer has provided sufficient funds in the payment account according to the bank's schedule. If the execution date is a non-business day, coverage must be provided on the payment account on the first following business day. The payer may instruct their bank to discontinue executing SEPA DD on their payment account. The payer's bank shall not execute SEPA DD in the event of insufficient funds in the payer's account, if the account is closed, if the payer has died, and if the execution of SEPA DD on the payer's account is prohibited or restricted. In the event of an unexecuted SEPA DD, the payer must settle the obligations towards the payee themselves.

The Bank shall not enable SEPA DD execution on the transaction account of a holder who is placed under guardianship.

3.10.2.3 Objection

The payer may deliver to their bank a written objection, requesting it not to execute individual SEPA DD transactions, 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. The payer may also express an objection to the recipient before the SEPA DD is executed in a manner and within the time limits agreed upon between them.

3.10.2.4 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.

The payer may request a refund of funds for already executed SEPA DD payment transactions:

- 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 of the execution date, 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 payer's bank receives proof of the existence of valid mandate, it shall reject the request for a refund. If the payer's bank receives from the payee'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 SEPA 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 SEPA DD no later than within thirteen (13) months also in the case of errors in the SEPA DD execution at the payer's bank.

Upon refund, the payer is entitled to interest at the €STR reference interest rate, which is calculated on the amount of the executed SEPA DD payment transaction from the day of execution of the SEPA DD up to and including the day before the day of refund to the payer's account.

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

3.10.2.5 Notifications

The payer shall be informed of the amount and the date of each individual SEPA DD by prior notification from the payee. The payer's 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 if the bank has it at its disposal at that time.

The payer shall be notified of executed SEPA DD payment orders by means of the payment account statement.

The Bank shall promptly inform the payer of any non-executed SEPA DD payment orders by a special notice in the manner agreed in the agreement.

3.10.2.6 Fees

The payer shall pay the payer's bank a fee for SEPA DD execution and non-execution in the manner and in accordance with the applicable Fee List. All fees related to SEPA DD will be directly debited from the payer's payment account, whereby the payer, by signing the Consumer Payment Services Agreement, expressly consents to this and irrevocably authorises the Bank to make such a debit.

3.10.3 Standing order

A standing order as a credit transfer is a payment service:

- By which the payer gives a written consent to the Bank to execute a single payment transaction in the domestic currency, repeated in the same amounts and executed on a specific date;
- By which the payer gives a written consent to the execution of a specific payment transaction in the domestic currency for the repayment of a liability to the Bank;
- By which the payer gives a written consent to the execution of a specific payment transaction in the domestic currency for transfers to savings in the same amounts, with the execution date being agreed in advance and the date of the last standing order also being determined;
- By which the payer gives a written consent to transfer the daily balance of the transaction account in the domestic currency to another account.

The Bank shall accept the consent for executing a standing order if the standing order is to be completed by at least two consecutive payments on a specific date in an agreed-upon chronological order.

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

The Bank shall not enable standing order and SEPA direct debit execution on the transaction account of a holder who is placed under guardianship.

3.10.4 Regular authorised ovedraft facility on the transaction account

An adult transaction account user agrees that the Bank, in accordance with the Bank's internal rules, may grant them a regular authorised overdraft facility in the amount of EUR 400.00. If the transaction account holder does not want the regular authorised overdraft facility, they may cancel it in writing. The transaction account holder shall not be charged a fee for the approval of a regular overdraft facility. A holder who has multiple transaction accounts with the Bank may only have an authorised overdraft facility on one account.

The Bank shall not enable overdraft facilities on the transaction account of a holder who is not of legal age and on the transaction account of a holder who is placed under guardianship.

If an extraordinary authorised overdraft facility is granted, the regular authorised overdraft facility shall be replaced by the extraordinary one.

The Bank shall charge interest for regular authorised overdraft facilities in a linear manner by considering the actual number of days in a month and the actual number of days in a year (365/366), in accordance with the applicable extract from the Bank's Capital Price List. The interest rate shall be reduced by 0.05 of a percentage point from the statutory default interest rate, set out in the Statutory Default Interest Rate Act, and shall change within the deadlines and in accordance with each change in the statutory default interest rate. In the event that the statutory default interest rate changes, the change shall enter into force at the same time as the new statutory default interest rate enters into force.

The transaction account holder shall pay interest monthly when they are accounted for and is obliged to provide funds in the amount of the accrued interest before its maturity in order to avoid an unauthorised negative balance.

The Bank has the right to unilaterally change the amount of the authorised overdraft facility or to disable the use of the regular overdraft facility. The Bank has the right to unilaterally cancel the regular authorised overdraft facility, in particular in the following cases:

- In case of an unauthorised overdraft on the transaction account;
- If the user has overdue liabilities to the Bank;
- When the user stops using their transaction account at the Bank;
- If there are no regular inflows to the user's transaction account for more than three (3) months;
- If it is notified of the user's death;
- If it receives a decision on an enforcement against the user. In such cases, the Bank may also unilaterally reduce the amount of the authorised overdraft facility or disable the use of the unused part of the authorised overdraft facility.

In the event of termination of the authorised overdraft facility, the user is obliged to immediately settle any unauthorised overdraft with the Bank.

3.10.5 Extraordinary authorised ovedraft facility on the transaction account

An adult account holder can request an extraordinary authorised overdraft facility on a transaction account based on a written application or via the digital bank. In the event of approval of the extraordinary authorised overdraft facility, the Bank and the account holder shall enter into a special agreement on the authorised overdraft facility on the transaction account.

3.11 Special debits of the transaction account

3.11.1 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 shall debit the user's transaction account based on a submitted bill if the bill contains a clause stating that the bill is payable at the Bank (domicile clause), if the bank account is not frozen due to enforcement, enforcement draft or outstanding liabilities to the Bank and if the Bank receives all the necessary information from the bill holder to cash the bill.

A bill is deemed to include an irrevocable authorisation of the user to the holder of the bill to order the execution of a payment transaction in accordance with the issued bill, and the irrevocable consent of the user to their bank to order the execution of a payment transaction against their funds.

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

In the event of receiving a decision on enforcement, securing of claims or other coercive intervention against the funds on the transaction account issued by a court, the Financial Administration of the Republic of Slovenia (FURS) or another competent authority, the Bank shall prevent the user from disposing of the funds in the transaction account (in the amount specified in the decision) and shall proceed in accordance with the operative part of the decision and 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 account user and the person designated as the creditor in the decision on enforcement or securing of claim.

The Bank shall charge a fee for the acceptance and execution of the decision in accordance with the Fee List applicable at the time.

3.11.3 Refund of overpayments to ZPIZ due to the death of a pension beneficiary

Upon receipt of a certificate of payment of benefits that were transferred by the Pension and Disability Insurance Institute (ZPIZ) to the credit of the user of the personal account after their death and to which the user was not entitled, the Bank shall, in accordance with the provisions of the Pension and Disability Insurance Act, return to the Institute the amount resulting from the certificate, but only within the scope of the positive balance in the account, based on the written request of the Institute.

3.12 Interest rates, fees and exchange rates

3.12.1 Transaction account interest rates

The Bank can pay interest on funds held in the transaction account at the interest rate for demand deposits, in accordance with the Decision on interest rates.

The Bank shall charge interest under this agreement in a linear manner by considering the actual number of days in a month and the actual number of days in a year (365/366). In determining the start and end dates of the interest accrual period, the Bank shall consider the first day after the agreement has been entered into, however, not the last day.

A change in the interest rate based on a change in the reference interest rate shall take effect immediately and without prior notice to the user. The user shall be informed in writing 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 in writing 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 shall be capitalised monthly upon calculation. The Bank shall notify the user of the amount of capitalised interest in the account statement.

The Bank shall charge interest on unauthorised debit balance on the transaction account in accordance with the Decision on interest rates.

3.12.2 Transaction account fees

The Bank shall charge the user fees for the payment services provided, as well as other services that it will perform in accordance with the Consumer Payment Services Agreement and these T&Cs, in the amount, deadlines and manner specified in the applicable Fee List. The Bank shall debit the user's account for the stated amounts, for which the user, by signing the Payment Services Agreement, gives the Bank a permanent and irrevocable order or irrevocably authorises it to make such payments to the user's transaction account.

The user shall pay the costs of reminders for any overdue liabilities in accordance with the Fee List applicable at the time,

default interest at the statutory default interest rate and other costs incurred with debt collection.

The user shall be notified in writing (e.g. in a statement) of any changes to the transaction account fees two (2) months before the change is introduced.

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 shall charge 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.

3.12.3 Exchange rates

In case of currency exchange, the Bank's exchange rate list valid at the time of actual exchange ("exchange rate list") shall apply, unless the contracting parties agree otherwise. The exchange rate list is published on the Bank's website www.otpbanka.si and at bank branch offices.

Payment transactions with a payment card executed in foreign currency shall be converted into EUR at the exchange rates of the card system (e.g. Visa Europe) applicable at the time of conversion. If the point of sale enables it, the cardholder has the option to choose whether to make the payment transaction in EUR via DCC or in local currency. DCC is not a service of OTP banka, but a service of the point of sale or ATM. In this case, the conversion rate and any additional costs are determined by the DCC provider. The Bank is not responsible for the costs charged by the DCC provider.

If the card is used to make payments in a currency other than EUR, the cardholder 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 on the same day may differ.

When executing payment transactions involving currency exchange in an EEA currency other than EUR, the Bank must provide payment cardholders with appropriate information in relation to currency conversion, including any percentage mark-up on the latest available ECB reference rate, to facilitate comparison of the exchange rates at which the bank issuing the payment card or the provider of instant currency conversion at ATMs or points of sale performs the conversion.

The percentage mark-up shall reflect the difference between the Visa exchange rate used and the latest available European Central Bank (ECB) reference rate.

The holder of the card with which the transaction was made will receive a message about the applied mark-up if the transaction is converted at the exchange rate used by the card issuer.

If the SMS Alert service is not activated for the card, a message about the mark-up on the ECB reference rate shall be sent to the mobile number that the Bank has in its system in relation to the payment card used.

If the SMS Alert service is activated for the card, the message about the mark-up on the ECB reference rate will be part of the received SMS alert message.

The user can unsubscribe from receiving this message at any time. More information about unsubscribing is published on the website otpbanka.si/kartice.

3.13 Informing the user about the balance and transactions on the transaction account

The user and the Bank may agree that the Bank will inform the user about the balance and transactions on the transaction account and about changes once (1) per month via the e-notification portal. To activate the e-notification portal, the user's email address is required.

If the user is a digital bank user, the Bank will inform the user about the balance and transactions on the transaction account and about changes once (1) per month via the digital bank.

Based on a form signed at any bank branch, the user may explicitly request that the Bank provide them with information on individual payment transactions carried out in paper form in an agreed manner, free of charge, once (1) per month. In case of 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 account holder’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 it is agreed to collect statements at the Bank, the user undertakes to collect the statements at the bank branch and is responsible for all consequences if the statements are not collected at the branch.

It is also deemed that holders of accounts in the name of a child are notified of changes in the balance and transactions on their personal account if their legal representatives are notified via the digital bank or the e-notification portal to the email address they provided to the Bank.

If the user receives statements via the e-notification portal to an email address, it is deemed agreed that the Bank will use the last email address provided for the above purposes. If the Bank receives an “undelivered email” message when sending a statement 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.

3.14 Termination of the agreement

The Consumer Payment Service Agreement shall end under the conditions set out in this section, unless otherwise specified in a specific subsection of section 3 of these T&Cs. The Consumer Payment Service Agreement may end 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 user and the Bank may mutually agree on the termination of the agreement. Such agreement shall be in writing.

c) With a notice of termination
The user may unilaterally terminate the agreement at any time in writing with a notice period of one (1) month.

The Bank may terminate an agreement concluded for an indefinite period of time with a notice period of two (2) months. The Bank shall provide the user with a notice of termination of the agreement in a clear and understandable manner on paper or another durable medium. The Bank shall send the notice of termination on paper to the user'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 Consumer Payment Service Agreement via a permanent data carrier.

In the case of termination of the agreement, the user shall pay the Bank the fees charged by the Bank for payment services for a certain period of time only in a proportional share until the agreement ends. If such fees are paid in advance, the Bank shall reimburse the user a proportionate share of the fee paid.

The Bank may not charge the user special fees due to the termination of the agreement if the user 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 Consumer Payment Service Agreement with immediate effect if:
- The user violates the provisions of the agreement and these T&Cs, especially in the case of overdue liabilities to the Bank;
- The user uses the transaction account for illegal operations or operations that are not in accordance with the indications of the user at the time of establishing the business relationship, or do not meet the conditions for establishing or maintaining the business relationship set out in the Bank's internal regulations;
- The user's operations are contrary to the tax regulations or regulations in the field of preventing money laundering and terrorist financing and other regulations;
- There has been misuse when opening a transaction account via electronic identification or the transaction account is being used for abusive purposes;
- There is a suspicion of the commission or attempted commission of a criminal offence by the user that is directly or indirectly related to business with the Bank or the misuse of Bank documentation.

The Bank shall provide the user with a notice of withdrawal from the agreement on paper or another durable medium. The Bank shall send the notice of withdrawal on paper to the user's last known address. In the event of withdrawal, the Bank shall close the user's transaction account within three (3) days from the date of submission of the withdrawal notice by mail or from the date of receipt of the withdrawal notice when the Bank transmits the withdrawal notice via a durable data carrier.

If the agreement is entered into remotely, the user has the right to communicate their intent to withdraw from the agreement without having to provide a reason for their decision or pay a contractual penalty, provided they do so within fourteen (14) days of the day when the agreement was entered into and in accordance with the provisions of the valid Consumer Payment Service Agreement. If the user withdraws from the agreement within the timeline referred to above, the Bank shall have the right the charge the user only a proportional part of the fee for services rendered.

4 SAVINGS ACCOUNTS

4.1 Savings account

4.1.1 Opening a savings account

The legal relationship between the Bank and the savings account holder arises on the date of signing the Savings Account Agreement. The Savings Account Agreement is concluded for an indefinite period of time.

A savings account can be opened by a saver who has reached the age of 15, alone or on their behalf and for their account by one or both parents together as legal representatives or the guardian whose right to open an account is based on a decision of the competent authority.

A savings account can be opened on behalf and for the account of a person up to 15 years of age (“child”) by one or both parents together as legal representatives or the guardian whose right to open an account is based on a decision of the competent authority.

A child cannot manage a savings account on their own. This is done on their behalf by the legal representative or guardian who opened the savings account in the child's name. A legal representative who has not opened the savings account may, during the term of the agreement, submit a request to manage this account only with the consent of the legal representative who opened the savings account in the child's name.

The legal representative shall lose the right to manage the saver's savings account when the saver gains full legal capacity.

4.1.2 Use of the savings account

The saver can access funds in the savings account at bank branches with a valid personal identification document or through the digital bank.

It is not possible to make payment transactions to and from the savings account.

4.1.3 Interest accrual

The Bank shall calculate interest on a linear basis and add it to the principal annually. Interest shall be calculated by considering the actual number of days in a month and the actual number of days in a year.

The Bank shall pay interest on savings account balance within the deadlines, in the manner and at the interest rate determined by the applicable Decision on interest rates, which is published in all bank branches and on the Bank's website otpbanka.si. The Bank shall credit the accrued interest at the end of the accounting period and upon termination of the savings account.

The Bank shall announce any change in the interest rate or method of interest calculation that will be to the detriment of the saver in good time before the intended change in writing or in another manner appropriate for banking operations, and will immediately notify the saver in the contractually agreed manner.

The saver has the right to object to the change referred to in the previous paragraph of this subsection until the date of entry into force of the change by submitting a written objection to the Bank stating that they do not agree with the change.

If an objection is made, the saver is deemed to withdraw from the agreement on the date of the announced change in the interest rate or method of interest calculation. In the event of the saver's withdrawal, the Bank shall calculate interest until the payout date at the last agreed interest rate.

If the saver does not object to the change in the interest rate or method of interest calculation by the effective date, it means that they agree with the change.

4.1.4 Authorised users

The saver or legal representative may authorise one or more persons to dispose of the funds in the savings account.

The provisions of section 3.3 of these T&Cs shall apply *mutatis mutandis* to the granting of authorisation, the scope of the authorised user's rights and the termination of the authorisation relationship.

4.1.5 Termination of the agreement

The saver and the Bank can mutually agree on the termination of the Savings Account Agreement. Such agreement shall be in writing.

The saver may terminate the Savings Account Agreement in writing at any time with immediate effect.

The Bank may unilaterally terminate the Savings Account Agreement in writing with a fifteen (15) day notice period in the following cases:

- When the saver does not meet the conditions for establishing or maintaining a business relationship set out in the Bank's internal regulations;
- Due to product discontinuation;
- If there has been a minimum balance in the savings account for the last twenty-four (24) months and there have been no transactions during that time;
- Based on measures and decisions of state and judicial institutions based on law.

The Bank shall provide the saver with a notice of termination of the agreement in the contractually agreed manner. The Bank shall send the notice of termination on paper to the saver'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.

If the Savings Account Agreement is concluded remotely, the saver has the right to notify the Bank within fourteen (14) days from the date of conclusion of the agreement that they are withdrawing from the agreement, without having to state the reason for their decision or pay any contractual penalties.

4.2 TRIPLE PLUS SAVINGS ACCOUNT

4.2.1 Opening a Triple Plus savings account

The legal relationship between the Bank and the Triple Plus savings account holder arises on the date of signing the Triple Plus Savings Account Agreement. The Triple Plus Savings Account Agreement is concluded for an indefinite period of time.

A Triple Plus savings account can be opened by a saver who has reached the age of 15, alone or on their behalf and for their account by one or both parents together as legal representatives or the guardian whose right to open an account is based on a decision of the competent authority.

A Triple Plus savings account can be opened on behalf and for the account of a person up to 15 years of age (“child”) by one or both parents together as legal representatives or the guardian whose right to open an account is based on a decision of the competent authority.

A child cannot manage a Triple Plus savings account on their own. This is done on their behalf by the legal representative or guardian who opened the savings account in the child's name. A legal representative who has not opened the savings account may, during the term of the agreement, submit a request to manage this account only with the consent of the legal representative who opened the Triple Plus savings account in the child's name.

The legal representative shall lose the right to manage the saver's Triple Plus savings account when the saver gains full legal capacity.

The Bank shall open a savings account for the saver with the first transfer from the personal account in the amount of at least EUR 50, which shall also be the minimum balance of funds in the savings account until the savings account is closed. The user shall make all further deposits/transfers to the savings account at the time and in the amounts of their own choosing, and can agree with the Bank to open a standing order.

The saver may withdraw their funds from the savings account or transfer them to their personal account or the account for which they are authorised if more than thirty-one (31) days have passed since the date of each deposit/transfer/interest accrual, up to the amount of the minimum balance of funds. The available balance includes all funds that the user has deposited into the savings account, together with accrued interest (except for the minimum balance of funds in the savings account), if these funds have been in the savings account for more than thirty-one (31) days.

4.2.2 Use of the Triple Plus savings account

The saver can access funds in the savings account at bank branches with a valid personal identification document or through the digital bank.

It is not possible to make payment transactions to and from the savings account.

4.2.3 Interest accrual

The Bank shall pay interest on each deposit in the savings account at a uniform nominal interest rate, which depends on the term of each deposit in the savings account. Doing so, it shall take into account an increasing scale of interest rates

(from A% to F%) based on the term of each deposit in the savings account and the date of withdrawal using the FIFO method.

The interest rate scale is divided into 6 levels, which are defined by the term of each deposit in the savings account. A uniform nominal interest rate is set for each of the levels. Interest on each deposit shall initially be accrued at a uniform nominal interest rate which applies to level 1. After the period specified for level 1 has expired, the deposit shall bear interest at the uniform nominal interest rate for the next level. At level 6, the saver can achieve the highest possible uniform nominal interest rate.

Structure of the interest rate scale:

Level	**Term of each deposit in the savings account**	**Uniform nominal interest rate**
1	from 1 day to 31 days	(A%)
2	from 32 days to 90 days	(B%)
3	from 91 days to 180 days	(C%)
4	from 181 days to 365 days	(D%)
5	from 1 year to 3 years	(E%)
6	more than 3 years	(F%)

The FIFO ("First In - First Out") method for calculating interest takes into account that the saver will deposit and withdraw savings to/from the savings account at different intervals and in different amounts.

Each deposit will be interest-bearing according to the scale for the period from the deposit date (First In) to the withdrawal date (First Out).

The funds saved in the savings account are reduced with individual withdrawals in the order of deposits into the savings account.

The annual interest accrued on the savings account is also interest-bearing according to the interest rate scale, the same as other deposits. On the date of conclusion of the agreement, the increasing interest rate scale specified in the agreement shall apply.

The interest rate scale may change during the savings period. The applicable interest rate scale is set out in the Decision on interest rates and published on the Bank's website

otpbanka.si/obrestne-mere-storitev and in its branches. The Bank shall inform the saver about the new interest rate scale at least 30 days before the change takes effect on the Bank's website otpbanka.si/obrestne-mere-storitev, through the digital bank or in a contractually agreed manner. If the saver does not agree with the new interest rate scale, which can be changed without concluding an annex to the agreement, they may withdraw from the agreement without a notice period and without paying a fee. The saver must submit the withdrawal from the agreement no later than the day before the specified date of entry into force of the change. If the saver does not withdraw from the agreement within this period, it is deemed that they agree with the changes.

4.2.4 Authorised users

The saver or legal representative may authorise one or more persons to dispose of the funds in the savings account.

The provisions of section 3.3 of these T&Cs shall apply *mutatis mutandis* to the granting of authorisation, the scope of the authorised user's rights and the termination of the authorisation relationship.

4.2.5 Termination of the agreement

The provisions of section 4.1.5 of these T&Cs shall apply *mutatis mutandis* to the termination of the Triple Plus Savings Account Agreement, unless otherwise specified in this section.

If the agreement is terminated by the saver, the termination shall take effect on the same day it is received by the Bank, but no earlier than the 32nd day from the date of the last deposit of funds into the savings account.
If the agreement is terminated by the Bank, the termination shall take effect on the 32nd day from the date of the last deposit of funds into the savings account or upon the expiration of the 15-day notice period, if more than 32 days have passed since the last deposit of funds into the savings account.

On the day the savings account is closed, the saved funds shall be transferred to the personal account specified by the saver in the agreement.

4.2.6 Interest taxation

Regarding the taxation of interest and the application of annual interest accrual, the provisions of subsection 4.3.5 of these T&Cs shall apply.

4.3 Individual Retirement Account

4.3.1 Opening an individual retirement account

The legal relationship between the Bank and the individual retirement account holder arises on the date of signing the Individual Retirement Account Agreement.
The Individual Retirement Account Agreement is concluded for a fixed period of time, as agreed in the agreement.

An individual retirement account can be opened by a saver who has reached the age of 15, alone or on their behalf and for their account by one or both parents together as legal representatives or the guardian whose right to open an account is based on a decision of the competent authority.

An individual retirement account can be opened on behalf and for the account of a person up to 15 years of age (“child”) by one or both parents together as legal representatives or the guardian whose right to open an account is based on a decision of the competent authority.

A child cannot manage an individual retirement account on their own. This is done on their behalf by the legal representative who opened the individual retirement account in the child's name or the guardian. A legal representative who has not opened the individual retirement account may, during the term of the agreement, submit a request to manage this account only with the consent of the legal representative who opened the individual retirement account in the child's name.

The legal representative shall lose the right to manage the annuity saver's individual retirement account when the saver gains full legal capacity.

4.3.2 Use of individual retirement account

It is not possible to make payment transactions from the individual retirement account.

4.3.3 Authorised users

The provisions of subsection 3.3 of these T&Cs shall apply *mutatis mutandis* to authorised users individual retirement accounts.

4.3.4 Termination of the agreement

The Individual Retirement Account Agreement may be terminated early by written agreement between the parties.

The Bank may unilaterally terminate the Individual Retirement Account Agreement with a fifteen (15) day notice period in the following cases:

- When the saver does not meet the conditions for establishing or maintaining a business relationship set out in the Bank's internal regulations;
- Due to product discontinuation;
- Based on measures and decisions of state and judicial institutions based on law.

The Bank shall provide the saver with a notice of termination of the agreement in the contractually agreed manner. The Bank shall send the notice of termination on paper to the saver'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.

In the event of termination of the agreement at the saver's request, the saver shall pays the costs in accordance with the applicable Fee List.

The Bank shall transfer the amount of the saved funds, together with interest, less any accrued early termination costs, to the account specified in the Individual Retirement Account Agreement or subsequently notified to it by the saver, no later than eight (8) days after the date of termination of the agreement.

4.3.5 Interest taxation

Interest received from cash deposits and savings shall be taxed in accordance with the Personal Income Tax Act (ZDoh-2). The return form for the assessment of personal income tax on interest, instructions for completing it, and more information are available on the website of the Financial Administration of the Republic of Slovenia.

If a saver (taxpayer) who is a tax resident of Slovenia concludes a savings agreement for a period longer than one year, they may claim annual interest accrual (tax base under Article 84 of the ZDoh-2). In this case, the saver is liable each year for any tax payment on interest accrued or earned during the tax year. The saver shall notify the Bank of the decision to enforce this provision upon conclusion of the savings agreement or at the latest by the end of the calendar/tax year in which the savings agreement was concluded, by submitting to the Bank a signed form, Notice of enforcing the tax base under Article 84 of the ZDoh-2 on interest on long-term deposits and long-term savings with banks and savings banks. The decision on (non)enforcement is valid until the end of the agreement.

In accordance with the Personal Income Tax Act, the Bank shall annually inform the saver about the interest earned from short-term savings for the previous tax year and from long-term savings if the depositor has opted for annual interest accrual. If the saver has not opted for annual interest accrual, the Bank shall inform the saver of the interest earned after the savings period has expired within the deadlines and in the manner set out in the applicable legislation.

4.4 ZA-TO! savings account

4.4.1 Opening a ZA-TO! savings account

The legal relationship between the Bank and the savings account holder arises on the date of signing the ZA-TO! Savings Account Agreement.

A ZA-TO! savings account can be opened by a saver who has reached the age of 15, alone or on their behalf and for their account by one or both parents together as legal representatives or the guardian whose right to open an account is based on a decision of the competent authority.

A ZA-TO! savings account can be opened on behalf and for the account of a person up to 15 years of age (“child”) by one or both parents together as legal representatives or the guardian whose right to open an account is based on a decision of the competent authority.

A child cannot manage a ZA-TO! savings account on their own. This is done on their behalf by the legal representative who opened the ZA-TO! savings account in the child's name or the guardian. A legal representative who has not opened the ZA-TO! savings account may, during the term of the agreement, submit a request to manage this account only with the consent of the legal representative who opened the ZA-TO! savings account in the child's name.

The legal representative shall lose the right to manage the ZA-TO! savings account when the saver gains full legal capacity.

4.4.2 Use of ZA-TO! savings account

It is not possible to make payment transactions from the ZA-TO! savings account.

4.4.3 Authorised users

The provisions of section 3.3 of these T&Cs shall apply *mutatis mutandis* to authorised users ZA-TO! savings accounts.

4.4.4 Termination of the agreement

The provisions of subsection 4.3.4 of these T&Cs shall apply *mutatis mutandis* to the termination of the ZA-TO! Savings Account Agreement, unless otherwise specified in this subsection.

If the ZA-TO! Savings Account Agreement is concluded remotely, the saver has the right to notify the Bank within fourteen (14) days from the date of conclusion of the agreement that they are withdrawing from the agreement, without having to state the reason for their decision or pay any contractual penalties.

4.4.5 Interest taxation

Regarding the taxation of interest and the application of annual interest accrual, the provisions of subsection 4.3.5 of these T&Cs shall apply.

5 DEPOSIT

5.1 Withdrawal from the agreement

The depositor cannot unilaterally withdraw from the Term Deposit Agreement before the expiry of the term deposit period, unless they do not agree to a change in the interest rate under the terms and conditions and in the manner agreed in the Term Deposit Agreement.

The Term Deposit Agreement may be terminated early by written agreement between the parties.

In the event of a written agreement on early termination of the agreement referred to in the previous paragraph, the Bank shall, for the duration of the deposit relationship until its termination, pay interest on the deposit funds at the interest rate and in the amount agreed upon in the Term Deposit Agreement, and the depositor shall be charged costs in accordance with the applicable Fee List.

The Bank shall transfer the amount of the saved funds, together with interest, less the calculated cost of early termination, to the account specified in the Term Deposit Agreement, or to the account specified by the parties in the agreement on early termination of the agreement, no later than eight (8) days after the date of the agreed termination of the agreement.

The Bank may unilaterally terminate the Term Deposit Agreement with a fifteen (15) day notice period in the following cases:

- When the depositor does not meet the conditions for establishing or maintaining a business relationship set out in the Bank's internal regulations;
- Due to product discontinuation;
- Based on measures and decisions of state and judicial institutions based on law.

The Bank shall provide the depositor with a notice of termination of the agreement in the contractually agreed manner. The Bank shall send the notice of termination on paper to the depositor'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.

If the Term Deposit Agreement is concluded remotely, the depositor has the right to notify the Bank within fourteen (14) days from the date of conclusion of the agreement that they are withdrawing from the agreement, without having to state the reason for their decision or pay any contractual penalties.

5.2 Interest taxation

Interest received from cash deposits shall be taxed in accordance with the Personal Income Tax Act (ZDoh-2). The return form for the assessment of personal income tax on interest, instructions for completing it, and more information are available on the website of the Financial Administration of the Republic of Slovenia.

If a depositor (taxpayer) who is a tax resident of Slovenia concludes a Term Deposit Agreement for a period longer than one year, they may claim annual interest accrual (tax base under Article 84 of the ZDoh-2). In this case, the depositor is liable each year for any tax payment on interest accrued or earned during the tax year. The depositor shall notify the Bank of the decision to enforce this provision upon conclusion of the Term Deposit Agreement or at the latest by the end of the calendar/tax year in which the agreement was concluded, by submitting to the Bank a signed form, Notice of enforcing the tax base under Article 84 of the ZDoh-2 on interest on long-term deposits and long-term savings with banks and savings banks. The decision on (non)enforcement is valid until the end of the agreement.

In accordance with the Personal Income Tax Act, the Bank shall annually inform the depositor about the interest earned from short-term deposits for the previous tax year and from long-term deposits if the depositor has opted for annual interest accrual. If the depositor has not opted for annual interest accrual, the Bank shall inform the depositor of the interest earned after the term deposit period has expired within the deadlines and in the manner set out in the applicable legislation.

6 SAFE DEPOSIT BOX

The Bank shall make a safe deposit box available to the lessee on the basis of the signed safe deposit box lease agreement (“agreement”).

If the lessee wishes to rent several safe deposit boxes, a separate agreement shall be concluded for each individual safe.

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

6.1 Lease duration

The safe deposit box lease agreement is concluded for an unspecified period of time or 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 shall inform 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.

6.2 Authorisation

The lessee of the safe deposit box may authorise one or more persons to use the safe deposit box. The authorised user may only be an adult, a natural person with legal capacity 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 shall cease to be valid upon written cancellation by the lessee of the safe deposit box, termination of the authorisation by the authorised user, death of the lessee of the safe deposit box or the authorised user, and in the event of termination of the safe deposit box lease agreement. The lessee shall revoke the authorisation on the prescribed form of the Bank. The revocation of the authorisation must be notarised if it is not signed in person in the presence of a bank employee.

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

The authorised user is obliged to immediately notify the Bank in writing of the death of the safe deposit box holder and to cease business with the safe deposit box on the day of the death of the safe deposit box holder. The Bank is not liable for any damage that would arise if, after the lessee's death, the authorised user continued to use the safe deposit box and the Bank did not receive notification of the lessee's death.

6.3 Safe deposit box keys

Each safe deposit box has two locks. After signing the agreement and paying the rent, the Bank shall give to the lessee one or two identical keys to the safe deposit box, which the lessee or the authorised user may use. The Bank shall have 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 shall be opened by simultaneous double unlocking, which means that it can be opened by the lessee or the authorised user by opening the first lock with the key received upon conclusion of the agreement, but a bank employee must simultaneously unlock the second lock with the bank key that is different from the lessee's.

The correct use of keys when unlocking and locking the safe deposit box, proper locking of the safe deposit box and careful safeguarding of the keys is the responsibility of the lessee or authorised user. 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 user'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 List 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 the authorised user. 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 List.

6.4 Safe deposit access card

The Bank shall issue to the lessee and the possible authorised users a card for access to the safe deposit box, with which, together with a personal identification document, 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 of 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.

6.5 Safe deposit access magnetic card

In branches where magnetic cards are used for access to safe deposit boxes, the Bank shall issue a magnetic card for access to the safe deposit box to each of the lessees and the possible authorised users.

The Bank shall grant access to the safe deposit box to the lessee or any authorised user by the lessee or the authorised user inserting their magnetic card into the reader and entering their personal identification number (PIN). The personal identification number (PIN) shall be determined by the lessee or the authorised user 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 the authorised user after receiving a written notification. The lessee shall pay for the issuance of the new magnetic card in accordance with the Fee List.

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 users. 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 List.

6.6 Access to the safe deposit box

Only the lessee or the authorised user shall have access to the safe deposit box during the business hours of the 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 user 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 death of the lessee, the Bank shall deny the authorised user access to the safe deposit box.

The Bank shall deny access to the safe deposit box to the lessee and the authorised user in the following cases:
- Failure to pay the rent for the safe deposit box or other liabilities under the safe deposit box lease agreement until all liabilities have been settled;
- Received decision from a court or other competent authority ordering the Bank to block the safe deposit box in accordance with the applicable regulations.

6.7 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.

6.8 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 shall confirm 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 subsection, 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 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.

6.9 Termination of the safe deposit box lease agreement

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

- The lessee has not paid the rent or other costs;
- The safe deposit box is used to keep items which may not be kept in it in accordance with subsection 6.7 of these T&Cs;
- The lessee did not allow the bank employee to check the contents of the safe deposit box in the case referred to in the second paragraph of section 6.7 of these T&Cs;
- The lessee or authorised user violates the provisions of the safe deposit box lease agreement or the provisions of these T&Cs.

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, set out in the Bank’s internal regulations.

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 or other costs are fully paid at the time of cancellation;
- The safe deposit box has previously been completely emptied;
- The lessee 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 of any authorised user;
- The lessee has notified the Bank of the cancellation in writing.

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

6.10 Death of the lessee

In the event of the lessee's death, the safe deposit box can be accessed by the heir who proves, through a final inheritance decision, that they have inherited the decedent's property. If there are more than one heir, the Bank shall grant access to the safe deposit box to a maximum of two, who have been authorised to do so by the other heirs on the basis of a notarised power of attorney. The heir must prove their identity with a valid personal identification document.

The heirs shall be granted access to the safe deposit box once any outstanding liabilities of the decedent relating to the rent for the safe deposit box and/or the costs of any forced opening of the safe deposit box and replacement of the lock and keys have been settled.

An heir who does not have a key to the safe deposit box or magnetic card is obliged to first pay the costs of damage caused by forced opening and replacement of the lock and keys or the costs of the magnetic card.

6.11 Items found

For items found in the premises where safe deposit boxes are located, the Bank shall prepare a report and act in accordance with the Rules on the procedure for handling found items (Official Gazette of the Republic of Slovenia no. 90/2015) or other regulations governing the handling of found items.

6.12 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 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 T&Cs.

If safe deposit boxes are moved to a new location due to the closure of the branch, the Bank shall provide the lessee with a safe deposit box at another location and the lease shall continue under the same terms and 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 such 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 section, it shall be deemed that the lessee agrees that the Bank can physically relocate the cabinet with safe deposit boxes and that the Bank shall not be liable for any damage to the contents of the safe deposit box.

6.13 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 exclusively 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 T&Cs.

The Bank shall not be liable for damage due to events beyond its control and in case of *force majeure*.

The Bank shall not be liable 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.

7 COMMON PROVISIONS

7.1 Deposit guarantee

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

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

The maximum deposit guarantee is EUR 100,000.00 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.

A credit balance in a fiduciary account is a deposit that, in the share belonging to an individual beneficial owner, is considered part of the deposit of that beneficial owner. The deposit is eligible for a guarantee only if the Bank has been provided with information to identify the beneficial owner. If information about the beneficial owners of the funds in the fiduciary account is not reported to the Bank, the credit balance in the fiduciary account is treated as a bearer deposit that is not eligible for the guarantee.

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

7.2 Sanctions

(1) “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:
a. United Nations Organisation;
b. European Union;
c. United States of America;
d. United Kingdom of Great Britain and Northern Ireland (HMT Treasury and Bank of England).

(2) “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.

(3) “Person under sanctions” means a person subject to sanctions.

(4) The Bank shall not enter into business relationships or carry out transactions with persons under sanctions. In addition, the Bank shall not enter into business relationships or carry out payment transactions with legal or natural persons directly or indirectly connected to Syria, Sudan, North Korea, Cuba, Iran, Myanmar or the area of Crimea, Donbass (Donetsk and Luhansk regions), 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 otpbanka.si/preprecevanje-pranja-denarja-cap-politika.

7.3 Management of daily balances

The Bank shall charge a fee for the management of daily 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 List. The fee shall be charged on the last day of the month for the current month.

The user irrevocably authorises the Bank to debit the user's personal account for the monthly fee for managing daily balances. If the user does not have a personal account, the user irrevocably authorises the Bank to debit their savings account monthly. The user undertakes to ensure that there is a sufficient balance for the payment of the fee for the daily management of balances. If the user does not have sufficient funds in their personal or savings account to pay the fee on the day the fee is payable, the Bank shall debit their personal or savings account immediately after the funds are received. The user agrees that the Bank may use any of their funds at the Bank to pay the fee.

7.4 User identification by phone

For the purposes of concluding an agreement over the phone as well as other activities performed over the phone, the user agrees that the Bank may identify them using personal security credentials of an appropriate level of reliability assigned to the user by the Bank for identification purposes (as a combination of letters, numbers or characters), as well as request other personal data from the user on the basis of which the user can be identified.

7.5 Digital user identification

Digital user identification ensures the identification of persons without their personal data using a video screenshot of the customer's face and a photo of a personal identity document, taking into account the prescribed procedure for the purposes of establishing and verifying the identity of a person in accordance with the applicable Money Laundering and Terrorism Financing Act and the Rules on technical conditions that must be met by secure remote-controlled or electronic procedures and means of identification.

During digital identification of a user, an audio and video recording of the face is created and stored, and the user uploads a copy of the front and back of their personal identity document. It is performed for computer comparison of the user's image in the recording and on the personal identity document.

In the process of digital user identification, the following shall be verified and assessed by computer and through a bank employee who confirms the identification:
- Matching previously entered customer data with the data on the personal identity document;
- Security features of the personal identity document;
- Logical consistency of all collected data;
- The appropriateness of the customer's stated purpose;
- Potential influence of third parties on the customer's will;
- The customer's response to questions and their behaviour during identification;
- Other data specified by applicable legislation on video identification.

In the process of digital user identification via video and electronic identification, the Bank shall process the following personal data:
- Name and surname;
- Address of permanent and temporary residence;
- Date and place of birth,

- Tax number;
- Nationality;
- Number, type and name of the issuer of the official personal identity document;
- Date of issue of the official personal identity document;
- Date of validity of the official personal identity document;
- The purpose of opening a personal account.

The Bank shall process the above data on the basis of the Prevention of Money Laundering and Terrorist Financing Act (ZPPDFT-2). Providing data is a legal obligation and if the user does not provide this data, the Bank may not open an account for them.
In accordance with Article 35 of the ZPPDFT-2 and the Rules on technical conditions that must be met by secure remote-controlled or electronic procedures and means of identification, the Bank must verify the user's identity in the digital identification process also by verifying biometric facial features from captured photographs and recordings. In this case, in addition to the data listed above, the Bank shall also process the following personal data:

- Date and time of identification;
- Video screenshots with the user's image and a photo of their official personal identity document;
- Biometric comparison of the user's image from a video screenshot and a photo of their personal identity document.

Biometric data processing shall be carried out based on the user's **explicit consent**. The processing of biometric data is a prerequisite for implementing remote electronic identification. If the user does not agree to the processing of biometric data, the digital account opening process cannot be completed. In this case, the account can be opened at any bank branch.
The Bank may terminate the user identification process via video call at any time if:

- The technical conditions do not allow for flawless identification, e.g. poor connection, poor image or sound, etc.;
- There is a suspicion that the personal identity document is not authentic;
- There is a suspicious circumstance in the process on the user's side;
- There is a likelihood of third party influence on the user's expressed will or the validity of consent.

The Bank shall store data obtained on the basis of the ZPPDFT-2 in the digital identification process for the entire duration of the business relationship between the user and the Bank and for ten years after the termination of the business relationship; it will store biometric data obtained for the purpose of confirming the user's identity for 6 months after confirming the user's identity.

7.6 Informing the Bank about changes

The user must notify the Bank of all changes to personal and other data, data on authorised users and other data relating to the account and specified in the agreement and other relevant documents and which are important for the implementation of the contractual relationship, no later than five (5) days from the date of the change. Such data includes, among other: change of name and surname, change of residence or address for sending statements, notifications, etc., change of employment, replacement of personal identity document, change of mobile phone number, change of email address and other data that the Bank must keep about the customer in accordance with the legislation and the Bank's internal regulations. Upon expiration of the validity of the personal identity document, the user must submit a copy of a new personal identity document to the Bank.

The Bank shall not be liable for any damage arising from the user’s failure to comply with the obligations regarding the notification of changes.

7.7 Sending notices or informing the user

If the account user is also a digital bank user, the user agrees that the Bank may serve all correspondence to them via the digital bank or the e-notification portal to the last email address provided.

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 Bank shall use the Bank's website otpbanka.si as a secure channel for informing payment service users in the event of suspected or actual fraud or security threats. For digital bank users, the notification shall be forwarded to the digital bank Inbox, and for e-notification users, to the e-notification portal. The Bank shall also notify users of suspected or actual fraud and scams via SMS or email, if the user has provided the customer with their mobile number or email address.

7.8 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.

7.9 Protection of personal data and confidential information

Information and data relating to the performance of payment services based on these T&Cs shall be treated as business secrets of the Bank. The Bank shall only disclose these data to the user of payment 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's transactions 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 Personal Data Protection Act, as detailed in the General Information on Personal Data Protection, available on the Bank's website otpbanka.si/vop 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 services:

- information about users of payment services 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 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 user and legal representative or guardian 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:

- Information about the user's job, profession and employer;
- Employment contract;
- Certificate of eligibility to receive a pension or annuity payment;
- Other documents demonstrating the source of income (e.g. proof of ownership of real estate);
- Valid school enrolment certificate;
- Residence permit and certificate of temporary/permanent address or other equivalent document;
- 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 services 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, 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 is aware that the personal data provided to the Bank, or which the Bank has in its databases, is processed and exchanged by the Bank for the purposes of fulfilling contractual obligations, recovering claims in the event of non-fulfilment of contractual obligations, in legal proceedings between the Bank and the user and other proceedings that the user or competent authorities may initiate against the Bank, as well as for the purposes of fulfilling the relevant legal and regulatory obligations of the Bank and obligations adopted and in accordance with international legal acts adopted by the Republic of Slovenia and acts of the European Union, and all binding domestic and international acts and rules that apply or relate to the prevention of money laundering and terrorist financing, and the implementation of the international agreement concluded between the Republic of Slovenia and the USA in relation to the Foreign Account Tax Compliance Act (FATCA), the OECD standard for the automatic exchange of financial account information (CRS - Common Reporting Standard) and the Tax Procedure Act (ZDavP).

Subject to relevant regulations, the Bank reserves the right to obtain a copy of an official personal identity document from the user and store it for the purpose of establishing and confirming the user's identity and implementing legal requirements

related to the correct identification of users.

The communication channels through which the Bank informs users are: regular mail, telephone, e-mail, SMS, digital channels (digital bank Inbox, push messages, notifications and messages via social or messaging networks (e.g. Viber, Facebook, Instagram ...), etc.).

An individual has the right to withdraw their consent for marketing purposes at any time or to object to the processing of personal data for marketing purposes.

7.10 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 T&Cs in an amicable manner.

A complaint or claim ("complaint") regarding a service provided by the Bank can be submitted to the Bank in person at any OTP banka branch or at specializsd bank counters in Pošta Slovenije units, or by mail to the Bank's address: OTP banka d. d., Slovenska ulica 58, 1000 Ljubljana, by email to reklamacije@otpbanka.si ali info@otpbanka.si, or to the toll-free phone number 080 17 70.

The Bank's first-instance body shall decide on the complaint within eight (8) days of receiving a complete complaint. The decision on the complaint shall be communicated to the customer in the agreed manner, except in the case of a rejected complaint, where the decision shall be communicated in writing. If the user disagrees with the decision of the first-instance body, they may file a written complaint against such decision to the Bank's addresses or email addresses listed above. They can also file a written complaint at any OTP banka branch or at a specialised bank counter of Pošta Slovenije. The complaint shall be handled by the second-instance body within the Bank.

The Bank's second-instance body shall decide on the complaint within fifteen (15) days of receiving a complete complaint.

When, in exceptional cases, due to reasons beyond its control, the Bank is unable to provide a response within the stipulated period, it shall inform the user of the status of the handling of their complaint and the date of the final resolution, which in no case shall be longer than thirty-five (35) days.

If the user, who is a consumer, does not agree with the decision of the Bank's second-instance body on the complaint or if they do not receive the Bank's response to the complaint within fifteen (15) days without justification, they have the right to initiate an out-of-court resolution of the dispute by regular mail to the Bank Association of Slovenia - GIZ, Šubičeva ulica 2, 1000 Ljubljana, phone: +386 1 242 97 00, with the note: initiative for out-of-court resolution of the dispute, on the website www.zbs-giz.si or by email to: izvajalec.irps@zbs-giz.si. The initiative for out-of-court resolution of the dispute must be submitted no later than thirteen (13) months from the Bank's final decision or if the client has not received a response within fifteen (15) days.

The mediation procedure is carried out by the competent authority of the out-of-court resolution provider in accordance with the rules of procedure of the out-of-court resolution provider and the act governing the out-of-court resolution of consumer disputes. More information is available on the website of the Bank Association of Slovenia at the link www.zbs-giz.si.

Despite the initiative to initiate an out-of-court resolution of the dispute, the user has the right to file at any time a lawsuit to resolve the dispute between them and the Bank before the competent court.

The Bank of Slovenia is responsible for conducting procedures for violations committed in connection with the provision of payment services.

Complaints regarding payments made by payment card
The Bank shall be responsible for resolving complaints regarding card transactions and providing information. In the event of a complaint, the cardholder shall contact the Bank unit that approved the issuance of the card, providing the appropriate documentation, The complaint shall be submitted in writing. The cardholder undertakes to remain available for contact through the contact details they have communicated to the Bank (email, 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 customer provides false statements in relation to the complaint, the Bank shall have the right to charge the holder the costs of the complaint. Complaints shall be resolved according to procedures laid down by the rules and instructions of licence holders – Visa card system and the Bank.

The cardholder shall notify the Bank of any unauthorised and/or incorrectly executed payment transaction as soon as they become aware that such reason for complaint has occurred, but no later than thirteen (13) months after the date of debiting the transaction account. The cardholder shall notify the Bank as soon as possible of any other disputes arising from card use where the cardholder 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 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 holder shall contact 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.

Complaints about the delivered content of the e-invoice
Any complaints arising from the content of e-invoice shall be resolved by the recipient of the e-invoice directly with the issuer of the e-invoice.
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-invoice.

Complaints about SEPA DD payments
The payer and the payee shall mutually resolve all complaints of the payer in relation to SEPA direct debits arising from their contractual relationship, whereas other complaints shall be resolved by the payer with the Bank.

Post office operations

The following bank products can be used at a post office counter:

- Transaction accounts;
- Savings account;
- Triple Plus savings account;
- individual retirement account; and
- ZA-TO! savings account.

The following payment transactions can be performed at the post office counter: payment of payment orders, withdrawals from transaction and savings accounts, deposits to transaction and savings accounts, internal transfers between accounts and savings accounts.
To use the services of the above products, the user needs a valid debit card and/or a valid personal identity document.

The following transaction accounts can be opened at the post office counter: Komplet Bundle, Ekstra Bundle, Personal Plus account, Youth Bundle, Prepaid (Net) account and Private individual transaction account.

7.12 Amendment and validity of the T&Cs

The following documents form an integral part of these T&Cs:
- The Bank's schedule for executing payment transactions (attached);
- Consumer Banking Fee List;
- Decision on interest rates relating to these T&Cs;
- General information on personal data protection and privacy statements for individual products and services; and
- General terms and conditions for using digitised cards in mobile wallets of other providers.

The Decision on interest rates, the applicable Fee List and the General information on personal data protection are available for viewing at the Bank's branches and on the Bank's website.

Before opening a transaction account, the user shall be provided with the necessary time, space and all available documentation required to open a transaction account and familiarise themselves with the content of the T&Cs. Before signing the agreement, the user shall be informed of the content of the T&Cs and, by signing the agreement, confirms that they understand them and fully agree with them.

If the account user is also a digital bank user, they agree that the Bank will forward the T&Cs to them via this channel.

If the account user is not a digital bank user, they agree that the Bank will send the T&Cs to their email address provided to the Bank; otherwise, the user shall receive the T&Cs on paper.

If the Bank amends these T&Cs, it must inform the user two (2) months before the changes come into effect by sending them a proposal for amendments to the T&Cs. The Bank shall inform the user about changes to the T&Cs in the manner agreed in the agreement.

If the user does not agree with the changes to the T&Cs, they may withdraw from the agreement without notice and without paying any fee. The user must submit the withdrawal from the agreement no later than the day before the specified date of entry into force of the change. If the user does not notify the Bank within this period that they do not agree with the changes, they shall be deemed to agree with the changes.

The T&Cs applicable at the time shall be published on the Bank's website and available to the user in all Bank's branches.

With the entry into force of these T&Cs, the previous T&Cs shall cease to apply. These T&Cs shall also apply to existing contractual relationships.

Provisions of the Consumer Payment Service 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 T&Cs and which are in conflict with the provisions of the ZPlaSSIED shall be considered to have been replaced by the provisions of the ZPlaSSIED.

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

The user has the right to request a copy of the agreement, the T&Cs and their integral parts on paper or another permanent data carrier at any time.

The law of the Republic of Slovenia shall apply to the provision of services in accordance with these T&Cs and their interpretation.

These T&Cs shall apply as of 1 December 2025.

OTP banka d.d.

8 APPENDIX: DOMESTIC, CROSS-BORDER AND OTHER PAYMENT TRANSACTIONS EXECUTION SCHEDULE

8.1 DOMESTIC PAYMENT TRANSACTIONS SCHEDULE

Payment type	Time of receipt by latest by	Execution guaranteed
Bank@Net/mBank@Net/Poslovni Bank@Net/Flik/Bank@Net.com, mBank@Net.com/eBank@Net.com		
Credit payments to account with OTP banka and settlement account of OTP banka (internal payments)	24/7	Same day
Credit payments to accounts with other banks in the Republic of Slovenia	16:00	Same day
Urgent payments SEK**	16:00	Same day
SEPA batch payments***	15:00	Same day
Instant payments	24/7	Same day
SEPA Direct Debits* via online bank**		
Under CORE scheme	07:00	D**** + 1 day
Under B2B scheme	07:00	D**** + 1 day
Objection (prior to execution of SDD)		D – 1 day
E-INVOICES via online bank		
E-invoices (delivery of e-invoices or e-return receipts to payee)	15:30	Same day (other than Sundays and holidays)
Bank counter		
Credit payments to account with OTP banka and settlement account of OTP banka (internal payments)	17:00*	Same day
Credit payments to accounts with other banks in the Republic of Slovenia	15:00*	Same day
Urgent payments SEK**	16:00*	Same day
Instant payments*	Branch office business hours	Same day
Cash deposit to account with OTP banka	17:00*	Same day
Cash withdrawal from account with OTP banka	17:00*	Same day
Delivery of bill of exchange for cashing to Enforcements unit	12:30	Same day

* The last time of receipt of payment orders depends on the business hours of the branch office.
** Urgent payments: only if expressly selected, priority treatment, shorter execution date, executed within 30 minutes.
*** Applies to entrepreneurs, private professionals, and corporates.
**** Bank business days MON, TUE, WED, THU, FRI by which the payee needs to provide data for SEPA DD. The payee can deliver the data by earliest 14 days prior to the scheduled debit date.

8.2 CROSS-BORDER AND OTHER PAYMENT TRANSACTIONS SCHEDULE

Payment type	Time of receipt by latest by *****	Execution guaranteed ***
Bank@Net/mBank@Net/Poslovni Bank@Net/Bank@Net.com, mBank@Net.com/eBank@Net.com		
Urgent payments**	10:00	Same day
Cross-border and other payments	15:00	Same day
SEPA batch payments (for private professionals and entrepreneurs)	15:00	Same day
SEPA Direct Debits* via online bank**		
Under CORE scheme	7:00	D***** + 1 day
Under B2B scheme	7:00	D***** + 1 day
Objection (prior to execution of SDD)		D – 1 day
Bank counter		
Urgent payments**	10:00	Same day
Cross-border and other payments	15:00*	Same day

* The last time of receipt of payment orders depends on the business hours of the branch office.
** Urgent payments: only if expressly selected, priority treatment for foreign currency subject to prior agreement by 10:00. Payments in currencies JPY, AUD, BGN and RON cannot be made as URGENT payments!
*** Execution of cross-border and other payment transactions to accounts of other banks (domestic or foreign) refers to the payment execution time in OTP banka, not the payment execution time in the other bank to the payee's account. OTP banka executes SEPA payments (received by 15:00), urgent payments, and other payment transactions to accounts with domestic banks on the same day and with the same execution date, whereas other cross-border and other payment transactions and SEPA payments received after 15:00 are executed on the same day and with the execution date of + one (1) business day.
**** Applies to entrepreneurs, private professionals, and corporates.

The payee can file a motion to object to the execution of an SDD on the value date or motion for a ban on the execution of an SDD one business day prior to the execution date. In order for an SDD to be executed, cash balances need to be available by 9:00 on the day of execution of an SDD.
A claim for a refund of an executed SDD needs to be made by no later than eight (8) weeks or thirteen (13) months (applies only to the CORE scheme).