SPECIAL BUSINESS TERMS AND CONDITIONS

Payment Institution NFD a.s.

1. INITIAL PROVISIONS

The Special Business Terms and Conditions (hereinafter referred to as the "SBTCs" or the "Agreement") of the Payment Institution NFD, a.s. company, registered office: Popradská 17/670, 064 01 Stará Ľubovňa, organization ID no.: 46 847 162 , registered in the Commercial Register kept by the Prešov District Court, section Sa, entry no. 10486/P, with the licence to perform activities as a payment institution registered under Decision no.: ODB-10851/2014-7 (hereinafter referred to as "NFD" or the "Company" or the "Provider"), form a part of each contractual relationship between the Payment Institution NFD, a.s. and the Client. The SBTCs regulate the relationships between the Payment Institution and the Beneficiary, set out the rules applicable to the use of payment facilities, and they are complementing and binding upon all parties to such a contractual relationship from the first day on which the Client manifests their will to establish a contractual relationship with the Company unless the parties expressly agree otherwise.

2. INTRODUCTION

The following contract terms and conditions ("Contract Terms and Conditions") represent a legal agreement between you and the Payment Institution NFD, a.s. company. ("Company", "us", "we") that regulates the use by you of our system intended for provision of payment services (directly or through contractors providing payment services) and other services as well as our internet banking and mobile banking systems ("Application" or "Software") and any version of our mobile application for provision of payment services.
To be able to make use of our Services, you have to accept these Contract Terms and Conditions to the full extent along with our personal data protection policy ("Personal Data Protection Policy") and by accepting these Contract Terms and Conditions you confirm that you have read and you understand and accept our Personal Data Protection Policy.

3. DEFINITIONS AND INTERPRETATION RULES

Provider of payment services – Payment Institution, the Payment Institution NFD a.s. company, registered office: Popradská 17/670, 064 01 Stará Ľubovňa, organization ID no.: 46 847 162.
Internet banking – a separate payment facility, private secured zone/environment on the Internet where the Client logs in and has the opportunity to fully use the payment services provided by the Provider.
Application – the BonoPay mobile application, payment application.
Mobil banking for iOS or Android: a separate payment facility, payment application for electronic banking, private secured zone/environment within a mobile network where the Client logs in and may use **selected** payment services provided by the Provider.
BonoPay E-Wallet - Mobile banking iOS or Android for the clients with personal or business accounts for cashless payment transactions with provision of selected payment services. Depositing or transfer of funds via single orders exclusively only to the extent of internal orders among users of payment services and this either to the e-mail of the Beneficiary´s client or with the possibility to read the QR code of the Beneficiary – Client by the Payer – Client, placing of payment orders for collection of funds from a payment card issued by other financial institution or bank in order to replenish the E-Wallet payment account serving to execute payments for purchase of goods and services.
BonoPay terminal - Mobile banking iOS or Android for the clients with merchant accounts for cashless payment transactions with selected payment services. Entering of payment orders to execute payment transactions involving collection of funds to receive payments for offered goods and services. Submission of payment orders to execute the payment transaction involving collection of funds from internal accounts only.
Selected payment services provided via the mobile application – account balance and transactions

overviews, Push notifications, invitation to friends to upload the application, list of the shops that are contractual partners of the Company, access to news, and as concerns the Merchant account – the application includes also the daily closing function and is limited so that it only accepts funds from Clients and displays the history of payments.

BonoCard module – a part of the BonoPay E-Wallet payment facility for iOS, Android included directly in the mobile application. It allows saving data of several payment cards, card preference selection, selection of a card for payment execution, securing of data via a special PIN code, and generation of QR codes based on the entered card data.

Registration within the mobile application: the process of creation of a profile within the BonoPay application for Clients of the Company in order to execute payments and receive funds upon successful registration and telephone number authorization via OTP and upon compliance with the KYC requirements. The KYC requirements are set out in more detail by the special AML regulation.

Payment gateway: a part of payment facilities, an internet interface available to Clients where it is possible to enter the Payer´s instruction while making use of the offered payment services provided by the Company either directly or through contractual payment service providers. The Company reserves the right to amend and update the range of offered payment services. Currently, the Company offers the following possibilities how to receive funds via the payment gateway: (i) via a bank transfer where only the banking data for the transfer of funds to a collection account of the Company are generated along with the unique identifier accompanying the payment, which the Client shall enter into the field "Payment Description or Variable Symbol; (ii) via the BonoPay terminal. It involves transfer of funds from the Client´s account to the Merchant´s account though an internal payment transaction. The internal payment is executed automatically after the Client is requested to enter their login data into the internet banking zone by which they confirm the order to execute payment that will be executed online; (iii) via the payment gateway of other contractual provider of payment services, i.e. card acquirer. For the transfer of funds from the payment card to the Client ´s personal or business payment account, the payment gateway of the eCard company is used. As concerns the internet application, the Client is re-routed to the web portal https://pay.ecard.pl where the Client enters the payment card number and its CVC code to execute the transfer. The Client communicates directly with the portal https://pay.ecard.pl of the Acquirer outside the IT structure of the Provider and therefore the Provider has no access to the entered data and the payment card. Communication is carried out using the secured http protocol, the portal certificate of the EV type, e.g. with enhanced verification, and is signed by the DigiCert certification authority. The payment gateway communicates within the secured payment account interface through the API gateway situated at ib.pay-institution.eu/gateway. The Payer selects from offered payment services a service provided either directly or indirectly by the Company; the responsibility for provision of the offered payment service is always assumed directly by the provider of the service in question. The scope of offered services and the fees associated with use of the offered services are specified in the Fee Tariff. When making use of individual payment services, the Payer has the opportunity to familiarize themselves with the terms and conditions applicable to the intermediated payment services; the terms and conditions applicable to the payment services provided directly by the Company are specified herein. Authorization of the Order entered by the Payer is secured by the payment service provider concerned to the extent and in the manner determined by the payment facility provider.

eCard: card acquirer - eCard Społka Akcyjna, 80 387 Gdansk, ul. Arkónska 11, mailing address: 00 043 Warszawa, ul. T. CZackiego 7/9/11.

One-time password (OTP) - a single generated SMS verification code sent to the mobile telephone/device in order to verify the authorization to use the mobile phone/device or for the purposes of authorization of the request entered by the Client within the internet banking environment.

Beneficiary: The person identified by the Payer as the recipient of the funds transferred within the payment transaction, the Client who has created a profile within the internal system with all particulars (name, surname, e-mail, telephone number, password) and opened a payment account with Payment Institution NFD to receive funds via payment transactions. The Beneficiary selects account type: Home (personal account), Business (business account), Merchant (business account for e-shops and regular shops). The Beneficiary having either personal or business account may, via the internet banking or the BonoPay E-Wallet, receive funds from other payment or bank account that is not kept by the Provider to the Beneficiary´s account kept by the Provider. The Beneficiary having the Merchant account may receive via the BonoPay terminal funds

from the Payers who have activated the BonoPay E-Wallet or receive funds via the internet banking from other payment or bank account kept under the name of the Beneficiary by someone else, not by the Provider. To avoid any doubts, the Beneficiary may act also as the Payer.

Payer: The Client who has created a profile within the internal system with all particulars (name, surname, e-mail, telephone number, password) and opened a payment account with Payment Institution NFD to execute payment/transfer funds via payment transactions. The Payer selects account type: Home (personal account), Business (business account), Merchant (business account for e-shops and regular shops). Via the BonoPay E-Wallet, the Payer may send funds only to those Beneficiaries who are Clients of the Company and have opened payment accounts with the Company. In addition to that the Payer may send via the internet banking funds to Beneficiaries regardless of whether they are or are not clients of the Company.

Client: a natural person or legal entity who has opened a payment account with the Company based on an agreement.

Payer´s order: an unequivocal payment order placed by the Payer or the Beneficiary, requesting the Company to execute a payment transaction.

Payment transaction: crediting, collection, or transfer of funds upon the Payer´s order or on their behalf via the Beneficiary´s order addressed to the payment service provider.

Funds: money, funds subject to cashless transfers.

Authorization of the Client´s order: confirmation of the Payer´s order by entering the OTP used within the internet banking service provided by the Company.

Provider: Payment Institution NFD a.s., registered office: Popradská 17/670, 064 01 Stará Ľubovňa, organization ID no.: 46 847 162, registered in the Commercial Register kept by the Prešov District Court, section Sa, entry no. 10486/P, with the licence to perform activities as a payment institution registered under Decision no.: ODB-10851/2014-7

Account: The payment account of the Payer and/or the Beneficiary kept by the Provider, in respect of which selected payment services are provided.

Card acquirer – other contractual provider of payment services who secures processing of the transactions carried out via the payment card and thus participates in the payment transactions of the Provider.

BonoPay service for the Payer – the Provider´s service making use of the E-Wallet that allows the Payer to enter payment orders from their payment account through the order to execute a payment transaction from the BonoPay application while the Payer is able to identify the Beneficiary via e-mail. Numbers of the payment accounts registered by the Provider are allocated to the e-mail addresses of the Payer and the Beneficiary. The BonoPay service for the Payer includes also the bonus program, push notifications, news, overview of the account balance and transactions, and lists of contractually bound Clients.

BonoPay service for the Beneficiary – the Provider´s service provided via the BonoPay terminal allowing generation of the QR code based on the payment data entered by the Beneficiary for Clients, i.e. amount, currency, payment description, which are to be read by the Payer via the BonoPay application; the service also displays text messages within the internet banking zone through mobile application PUSH notifications and allows replenishment of the E-Wallet from other account.

Beneficiary receiving payments – company (Merchant): The natural person or legal entity who supplies goods or provides services based on a trade licence. The Beneficiary receiving payments addressed to companies has a profile within the BonoPay system and an account kept by the Provider.

Payments to companies: payment orders executed by the Payer and intended for the Beneficiaries receiving the payments addressed to companies - entrepreneurs for the goods or services provided by the Beneficiary receiving payments addressed to companies (Merchant).

Bonus program – a program of discounts on fixed fees for executed and received payments in compliance with the special terms and conditions agreed in an amendment to the Master Agreement with the Beneficiary – Client who is not a consumer.

Chargebacks: individually agreed fees for making use of the BonoPay terminal between the Provider and the Beneficiary receiving payments addressed to companies (Merchant), which the Provider uses to cover the costs associated with the Bonus Program.

Service Termination – cancellation of the BonoPay service through permanent deletion of the Client´s profile and closing of the account.

Blocking of the BonoPay Service – blocking of the payment account to prevent any real and/or potential

abuse of the BonoPay services, which the Client may execute either via the private internet banking zone or the Provider´s helpdesk. No payment transaction execution orders may be placed during the temporary blockage.
Helpdesk – The contact department for Clients of the Company.
Mobile phone/device: a device owned by the Client and selected by the Client to make use of the mobile banking application.
AAE – authentication and authorization elements.

4. TERMS AND CONDITIONS FOR USE OF THE BONPAY TERMINAL TO RECEIVE PAYMENTS

1. Registration of the Beneficiary and entering into the Master Agreement give rise to the legal relationship between the Beneficiary and the Provider. In connection with the Master Agreement, the business client selects the possibility to receive and process payments via the BonoPay terminal and signs the agreement on acceptance and processing of payment transactions and provision of the payment facility – BonoPay terminal. This beneficiary is called Merchant.

2. The Merchant provides the Provider with their name, surname, e-mail address, telephone number, and permanent residence address and may enter, on a voluntary basis, the payment card data within the profile zone. The Provider allocates the payment account number to the Merchant for the purposes of identification of the Beneficiary (Client - Merchant).

3. The Merchant shall enter true, complete, and current data when registering. The Provider checks the telephone number holder via the ITP mechanism. They check the name and surname based on submitted supporting documents serving to verify the payment account. E-mail address is checked as well. The Merchant shall enter the PIN that they will use to access the payment facility.

4. The Beneficiary – Merchant agrees that where the Payer provides e-mail address for execution of a payment transaction, the Payer´s payment account number will be the account number registered with the Payer´s e-mail for the purposes of payment order processing.

5. The Provider provides the Beneficiary with the BonoPay Service via the payment facility entitled BonoPay virtual terminal.

6. Via the payment facility - BonoPay terminal, the Beneficiary carries out cashless payment transactions – collection of funds in favour of the payment account of the Client – Beneficiary - by generating the QR code along with a description of payment data by the Beneficiary for the Payer – Client, enters payment orders to collect funds - payments for offered goods and services; the Beneficiary enters payment orders to execute the payment transaction involving collection of funds from internal accounts only, which means internal transfers between the users of payment services who are clients of the Payment Institution.

7. The Merchant understands and accepts that their account number saved within the profile will be displayed within the transaction details available to the Payer.

8. The Merchant understands possible consequences that they will bear if they state untrue and/or inaccurate data, in particular, an incorrect amount and/or currency, which will result in processing of the payment transaction using the incorrect amount and/or currency. Where the Beneficiary enters an incorrect amount and/or currency in their payment order, the Payer may request that the Provider return the payment.

9. The Provider shall use the Merchant´s e-mail address to inform about any change in the Merchant´s profile data and throughout the process of private zone password renewal.

10. The Merchant enters the text of requested mobile application push notifications via the internet banking.

11. The Merchant shall refrain from abusing push notifications to send threatening, bothering, or unethical texts as notification messages to other application users. The Beneficiary understands that the Provider is entitled to decide at their own discretion whether the content of the text entered by the Beneficiary in push notifications within the mobile application is published or the service is blocked for the Merchant.

12. The Merchant shall terminate their profile upon loss of control over their mobile device, e-mail address or telephone number or forthwith request change of the e-mail address and/or telephone number.

13. The Merchant shall update the information contained within the profile, the Provide shall bear no liability for the damage that occurs due to the Beneficiary´s fault.

14. The Provider reserves the right to terminate provision of all service that the Provider provides the Merchant with where the Merchant violates in any manner any provision of the Special Business Terms and Conditions.

5. TERMS AND CONDITIONS APPLICABLE TO THE USE OF BONOPAY – E-WALLET TO EXECUTE PAYMENTS

1. Registration and entering into the Master Agreement give rise to the legal relationship between the Payer and the Provider. BonoPay – E-Wallet provided by the Provider to the Payer is intended exclusively only for those Payers who have either personal or business accounts with the Provider (hereinafter referred to as the "Payer").

2. The Payer provides the Provider with their name, surname, e-mail address, telephone number, permanent residence address and may enter, on a voluntary basis, the payment card data within the profile zone. The Provider allocates a payment account number to the Payer for the purposes of identification of the Payer.

3. The Payer shall enter true, complete, and current data when registering. The Provider checks the telephone number holder via the OTP mechanism and they check the name and surname based on submitted supporting documents serving to verify the payment account. E-mail address is checked as well. The Payer shall enter the PIN that they will use to access the payment facility.

4. The Provider provides the Payer with services via the payment facility – BonoPay – E-Wallet.

5. Via the BonoPay - E-Wallet payment facility, the Payer carries out cashless payment transactions – crediting or transfer of funds via single orders exclusively only to the extent of internal orders among users of payment services and this either to the e-mail of the Beneficiary - Client or by reading the QR code generated by the Beneficiary – Client; the Payer may place payment orders for collection of funds from a payment card issued by other financial institution or bank in order to replenish the payment account serving as an E-Wallet for payments for purchase of goods and services. The payment facility offers also the possibility to withdraw funds from the payment card.

6. The Merchant understands and accepts that their account number saved within the profile will be displayed within the transaction details available to the Payer.

7. The Payer understands possible consequences that they will bear if the Merchant states untrue and/or inaccurate data, in particular, an incorrect amount and/or currency, which will result in processing of the payment transaction using the incorrect amount and/or currency. Where the Beneficiary enters an incorrect amount and/or currency in their payment order, the Payer may request that the Provider return the payment.

8. The Provider shall use the Payer´s e-mail address to inform about any change in the Payer´s profile data and throughout the process of private zone password renewal.

9. The Payer may receive mobile application push notifications.

10. The Merchant shall refrain from abusing push notifications to send threatening, bothering, or unethical texts as notification messages to other application users. The Beneficiary understands that the Provider is entitled to decide at their own discretion whether the content of the text entered by the Beneficiary in push notifications within the mobile application is published or the service is blocked for the Merchant.

11. The Payer shall terminate their profile upon loss of control over their mobile device, e-mail address por telephone number or forthwith request change of the e-mail address and/or telephone number.

12. The Payer shall update the information contained within the profile zone; the Provider shall bear no liability for the damage that occurs due to the Beneficiary´s fault.

13. The Provider reserves the right to terminate provision of all services that the Provider provides the Payer with where the Payer violates in any manner any provision of the Special Business Terms and Conditions.

6. TERMS AND CONDITIONS APPLICABLE TO THE USE OF BONOPAY – E-WALLET TO REPLENISH THE E-WALLET – THE BONOCARD MODULE

1. The Provider provides the Payer with the possibility to replenish the E-Wallet from other payment card.

2. The Provider provides the Payer with the BonoCard module.

3. The BonoCard module allows saving of data of several payment cards, card preference selection, card selection for payment execution, data securing via a special PIN code, and generation of QR codes based on entered card data. The card data saved within the BonoCard module, i.e. within the secured environment of the BonoPay application, are not saved within the server of the Company - Provider but they are administered exclusively only by the Client and protected by a special PIN code within the Client´s own mobile device – the Client is the user of the payment facility.

4. The service involving replenishment of BonoPay – E-Wallet for Clients with either personal or business account as a part of the payment facility “Mobil banking for iOS, Android” is located directly within the mobile application in the section “Accept money/Replenish the Wallet via the Payment Card”. It allows uploading of the payment card data directly within the payment gateway of the card acquirer – the eCard company that is another entity participating in the payment transactions of the Payment Institution - the Provider. The Client shall enter a QR code containing the payment card data via the BonoCard module.

5. After logging into the own mobile application BonoPay and entering the PIN, the Payer – Client has direct access to the card data saved in the BonoCard module as a QR code that the Payer will use to commence the process of a transfer from other bank account of the Payer (who is the Client of the Payment Institution with a business or home account) to the payment account of the Beneficiary (Client) kept with the Payment Institution and located within the environment of the card acquirer.

7. TERMS AND CONDITIONS APPLICABLE TO THE USE OF INTERNET BANKING

1. Internet banking – a separate payment facility, private secured zone/environment on the Internet where the Client logs in and has the opportunity to fully use the payment services provided by the Provider or administer their profile data based on the Master Agreement.

2. Upon registration, the Client selects the login name and password for access to the internet banking zone.

3. Via the internet banking zone, the Client may execute cashless payment transactions – transfers of funds via a single or standing payment order, domestic payment orders, foreign payment orders, SEPA payments, internal transfer orders to an account of the account holder denominated in other currency (the relevant foreign currency is sold by the bank that administers accounts for Payment Institution NFD a.s.), internal orders among users of payment accounts, receipt of funds and this: (i) via a bank transfer where only banking data for transfer of funds to the Provider´s collection amount (the Payment Institution company) are generated; (ii) via the payment gateway of other contractually bound provider of payment services, i.e. card acquirer. For the transfer of funds from the payment card to the Client´s personal or business account or to the Merchant´s account, the payment gateway of the eCard company is used. As concerns the internet application, the Client is re-routed to the web portal https://pay.ecard.pl where the Client enters the payment card number, expiry date, and its CVC code to execute the transfer. The Client communicates directly with the portal https://pay.ecard.pl of the Acquirer, outside the IT structure of the Provider and therefore the Provider has no access to the entered payment card data. Communication is carried out using the secured http protocol, the portal certificate of the EV type, e.g. with enhanced verification and signed by the DigiCert certification authority. The payment gateway communicates within the secured payment account interface through the API gateway that is at ib.pay-institution.eu/ gateway. Authorization of the Order entered by the Payer is secured by the payment service provider concerned, i.e. eCard – the card acquirer, to the extent and in the manner determined by eCard.

4. The Client uses an SMS code generated to the registered and verified e-mail address or registered verified phone number of the Client for authentication purposes within communication with the Payment Institution.

5. Via the internet banking, the Client may complement or change the profile data, i.e. change of name, surname, title, change of the registration or service e-mail address, IBAN for transfer of possible liquidation balance, address, identity card, password, and language and currency, may enter modifications of standing orders and payment templates, enter and request publication of a text message via PUSH notifications within the BonoPay mobile application, block the payment account or terminate it and in addition to that the Client has access to the history of payments, ordered payments, history of the payments that have not been executed, entered standing orders, entered payment templates, and history of currency exchange transactions.

6. Each logging into the internet banking zone via a new device is notified to the Client via a notification e-mail message containing the login date and time.

8. TECHNICAL REQUIREMENTS APPLICABLE TO SMARTPHONES AND TABLETS

- operating system iOS or Android (version 9.0 or higher) or Android (version 6 and higher)
- user accounts within App Store and Google Play
- internet access

The Payment Institution reserves the right to incompatibility of the application as concerns non-standard types of smartphones and tablets.

9. DATA PROTECTION

The Client shall:

a) prevent any abuse and/or unauthorized use of the mobile device with the registered e-mail address and telephone number. Upon loss or theft of the mobile device, the SIM card shall be blocked immediately via the mobile operator and the Provider´s helpdesk service shall be contacted as well.
b) protect the login name and password or PIN to the BonoPay application against disclosure, making

them available or other unauthorized provision. Upon any suspected disclosure of the password, the Client shall forthwith change it and check all the data in their BonoPay profile via the mobile application or the internet banking zone. Where the password cannot be changed, the Beneficiary shall contact the Provider´s helpdesk without undue delay.

c) protect the access to the entered e-mail address and thus prevent abuse of the data sent via the BonoPay service, in particular, the data serving to renew the private zone password.

The Provider shall not be liable for:

a) truthfulness and accuracy of the data entered in the BonoPay application. The Payer and the Beneficiary shall be liable for the truthfulness and accuracy of such data;
b) abuse of the mobile device of the Payer or the Beneficiary;
c) abuse of the data that the Payer and the Beneficiary shall protect.

10. SAFE USE OF PAYMENT FACILITIES, THEIR BLOCKING AND LIABILITY FOR PAYMENT TRANSACTIONS

1. The Client shall use the payment facility and individual authentication and authorization elements in compliance with the terms and conditions set out in the GBTCs and these SBTCs. After defining authentication and authorization elements (AAE) and after payment facilities are made available, the Client shall take all reasonable measures to safeguard their protection and protection of the payment facility; according to the Payment Institution´s opinion, its experience and practice in this area are to be factored in as reasonable and the Client shall, in particular:
   a) not leave AAE unattended and shall prevent any disclosure of AAE or making them available,
   b) handle AAE and individual payment facilities with the same care as when using a real wallet containing cash and shall not leave them freely available or accessible when the owner is not present,
   c) refrain from using the password and other AAE to access payment facilities within other systems (e.g. social networks, etc.),
   d) not write down or otherwise record the password, PIN, and other AAE for the access to payment facilities and shall refrain from providing them to any third party, including the police and the Payment Institution´s staff,
   e) not leave the written password or PIN close to a computer, mobile device or other technical equipment serving to make use of the services provided via electronic communication channels,
   f) no password, PIN or other AAE may be in the form of a simple sequence of characters (e.g. 1234, 1111, 0000, etc.) or a word that is easy to identify. Similarly, when defining and changing the PIN code, no easily identifiable combinations should be used (e.g. date of birth, last four digits of the birth number, or simple numerical progression, etc.),
   g) after execution of all required steps, the Client shall always to log out and close the internet banking and the application within the mobile device,
   h) not log into the internet banking zone via public or unknown computers,
   i) use connections only via secured WIFI networks or the data services provided by telecommunication operators,
   j) not log into the internet banking zone using a link in an e-mail message or within other web sites except for the web site of Payment Institution NFD a.s.,
   k) check the security of the connection to the internet banking zone based on the URL address https://ib.pay-institution.eu/web/ sign/auth and the valid certificate issued for Payment institution NFD, a.s.,
   l) use duly licensed antivirus and anti-spy software with the latest updates,
   m) refrain from downloading into the mobile device and using other than certified applications from the relevant application store, e.g. iTunes Store, Obchod Play, App Store, Google Play,
   n) upon installation of relevant application BonoPay (small) and upon its updates, the Client shall check the issuer of the application, i.e. Payment Institution NFD a.s. and the application developer, i.e. K_CORP s.r.o.,
   o) refrain from decompiling the application specified in sub-clause (xiv) of this clause, from reverse engineering, and from modifying it,

p) check the sender of the authorization SMS for access to electronic services,
q) regularly update the application specified in sub-clause (xiv) of this clause so that its latest version is used to safeguard security and remove defects,
r) regularly update the mobile device software so that the latest available version of the operating system is used,
s) upon loss of the mobile device, the helpdesk of the Payment Institution NFD shall be contacted immediately.

2. Where the Client believes that either the payment facility of AAE may be abused, the Client shall contact the helpdesk of the Payment Institution NFD at helpdesk@pay-institution.eu using the Client´s registered e-mail address or via the telephone number +421(0)911 052 118, Call-centre +421(0)52 46 810 89 and request blocking of the access. The Client shall proceed similarly in case of loss or theft of AAE or the mobile device.
3. The Payment Institution shall be entitled to block the use of the payment facility or AAE even without the Client´s request:
   a) based on the grounds involving security of the payment facility and payment services,
   b) due to a threat of unauthorized or fraudulent use of the payment facility and payment services,
   c) due to suspected violation of the obligations specified in these SBTCs.
4. The Payment Institution monitors behaviour of Clients using both automated and manual methods and the Payment Institution reserves the right to block AAE or the payment facility where the Payment Institutions determines that the Client´s behaviour is non-standard.
5. The Payment Institution shall inform the Client about blocking of the payment facility before blocking AAE or the payment facility or immediately after blocking them and this in an appropriate manner determined by the Payment Institution.
6. If the Client establishes an unauthorized or incorrectly executed payment transaction, the Client shall be entitled to a corrective action by the Payment Institution provided that the Client informs, without undue delay from the date of establishment of the unauthorized or incorrectly executed payment transaction but no later than within 13 months from deduction of funds from the account concerned or crediting of funds to the account concerned, the Payment Institution about the fact that the Client established the unauthorized or incorrectly executed payment transaction giving rise to the Client´s entitlement to a corrective action. Due to the fact that the above specified payment transactions may be linked with a crime (e.g. fraud, damage to and abuse of information media records, theft) or may give rise to damage or unjust enrichment, the Client shall provide, when informing the Payment Institution about any detected unauthorized or incorrectly executed payment transaction, the Payment Institution with maximum possible cooperation within establishment of causes and consequences of such payment transactions.
7. The Client who is a consumer under these SBTCs or the Payment Services Act shall bear the loss amounting to EUR 50 in relation to all unauthorized payment transactions, which los is caused by use of a stolen or abused payment facility by an unauthorized person due to the Client´s negligence as concerns protection of identification, authentication, and authorization elements (AAE). Despite the fact that the Client is a consumer under these SBTCs or the Payment Services Act, the Client shall bear all the loss associated with unauthorized payment transactions where they have been caused by fraudulent actions of the Client, a wilful failure to comply with one or several obligations under clauses 1 and 2 of this Article of the SBTCs or a failure to comply with one or several obligations under clauses 1 and 2 of this Article of the SBTCs due to gross negligence. The Client – consumer shall bear no financial loss resulting from the use of a lost, stolen or abused payment facility: (i) after the delivery of the notice under clause 2 of this Article except where the Client acts in a fraudulent manner; (ii) where the Client could not establish the loss, theft, or abuse before execution of a payment transaction except where the Client acts in a fraudulent manner; (iii) where the financial loss is caused by actions or negligence of an employee of the Payment Institution; (iv) where such a payment transaction occurs after the effective date of Section 3(c) of the Payment Services Act and despite that the Payment Institution fails to request strong authentication from the Client or applies an exception from the strong authentication, saving the cases where the Client acts in a fraudulent manner.

11. BONOPAY SECTIONS

A: Sections of the BonoPay terminal for acceptance of payments – the Merchant version

1. 7 sections are displayed after starting the application: “News”, “Accept Money”, “Accounts”. “Balance the Accounts”, “Invite Friends”, “Discount Points”, and “Partner Shops”.

2. The section “News” contains information about current issues and is provided to all application users.

3. The section “Accept Money” allows acceptance of funds to the payment account of the Beneficiary or Client. Sub-section “Via mobile phone” serves to accept money via the mobile phone by the Beneficiary as the acceptance point of the BonoPay application while the Beneficiary – Client enters “Amount”, “Currency”, and “Payment description” in respect of the payment account kept by the Company. After confirming the data, a QR code is generated within the BonoPay application of the Beneficiary - Client to be read by the Payer - Client. The Payer sends funds with the identifier of the Beneficiary receiving payments addressed to companies, which is entered via the QR code. The Beneficiary receiving payments addressed to companies is responsible for issue of the QR code containing their identifier. Sub-section “Payment Description” allows the Beneficiary to enter a note – a short text that may contain, for instance, the reason behind the acceptance of funds, etc. The maximum number of characters for such a note is limited.

4. One BonoPay Terminal is assigned to one Merchant payment account or one Merchant account may have a network of branches, which subsequently enables the Merchant to create several subaccounts.

5. The section “Accounts” contains information about your payment account balance and the amount of reserved balance, ordered payments, and fees. It allows cancellation of a payment within a certain period of time.

6. The section “Balance the Account” contains information about all payments received via the BonoPay application.

7. The section “Discount Points” contains information about allocated discounts on fees.

8. The section “Invite Friends” allows inviting other natural person or legal entity to register via the mobile application.

9. The section “Partner Shops” contains a list of contractual users of the mobile application along with their geographical locations.

B: Sections of BonoPay – E-Wallet – the version for Personal and Business accounts

1. It contains 7 sections: "News", "Pay by Mobile Phone", "Replenish Wallet", "Accounts", “Discount Points", "Invite Friends", "Partner Shops" and the BonoCard module.

2. The section “News” – see clause 5(b).

3. The section “Pay by Mobile Phone” allows the Payer to execute a payment to the Client´s e-mail address or pay by reading the QR code from the BonoPay mobile application of the Beneficiary receiving payments or the Beneficiary receiving payments addressed to companies for goods and services.

4. The section “Replenish Wallet” allows the Payer – Client to replenish the E-Wallet via the payment card issued by other payment institution or bank.

5. The section “Accounts” – see clause 5(h).

6. The section “Discount Points” contains information about allocated discounts on fees.

7. The section “Invite Friends” – see clause 5(k).

8. The section “Partner Shops” – see clause 5(l).

12. FINAL PROVISIONS

1. The Payment Institution hereby gives the Client consent to use payment facilities. The granted consent is non-exclusive, non-transferable to any third party, and is limited in time, i.e. until the time when the Payment Institution closes the payment account regardless of the reason. The Client is entitled to use payment facilities in the manner resulting from the purposes for which they are intended. The above consent applies also to all future versions and updates of payment facilities where such versions and updates are provided by the Payment Institution or its contractor. Payment facilities contain the trade secret and know-how of the Payment Institution and/or its contractor and therefore they are subject to intellectual property rights belonging to the Payment Institution and/or its contractor. The User is not entitled to amend, modify, or complement the application, to duplicate, process, change, distribute it, to translate the application from the absolute code to the source language, to freely modify or adapt the application at the Client´s discretion and this not even through third parties. Furthermore, the user is not entitled to create a backup copy of the application and this not even through third parties because such a copy is not required for functioning and use of the application. The user is not entitled to examine or test the functioning of the application in order to discover the principles based on which it was established and developed, including any application element.

2. These SBTCs have been drawn up in the Slovak language and in compliance with laws of the Slovak Republic.

3. The Payment Institution shall be entitled, depending on amendments to generally binding legal regulations and/or at own discretion, to amend or fully replace these SBTCs. The Payment Institution will publish such amendments via its web site or in another manner along with specification of the dates of validity and effect of such amendments. If an updated wording of the SBTCs does not contain the dates of validity and effect, the amended/new wording of the SBTCs shall take effect on the first day of the second month following their publication. The Payment Institution undertakes to publish any possible amendments no later than 2 months before the effective dates of relevant amendments. If the Client does not accept an amendment to the SBTCs, the Client is entitled to notify their non-acceptance within 30 days from the date of publication of the amended SBTCs – a timely notice of non-acceptance of the published wording of the SBTCs shall have a suspensory effect as concerns objected provisions for the Client who notifies such non-acceptance. In such a case, the Client shall be entitled to withdraw from the Agreement. If the Payment Institution and the Client fail to agree otherwise within 30 days and the Client does not withdraw from the Agreement, the amended – current wording of the SBTCs shall apply to the Client in compliance with all implemented changes. If the Client fails to notify the Payment Institution about the Client´s non-acceptance of an amendment to the SBTCs within the above specified period of time, it shall be believed that the Client accepts the amendment and the mutual relationships between the Payment Institution and the Client shall be governed by the amended SBTCs commencing from the effective date thereof.

Effective on April 20th, 2020.