



GENERAL TERMS FOR THE USE OF PBZ DIGITAL BANKING FOR BUSINESS ENTITIES

1. INTRODUCTORY PROVISIONS

1. These General terms for the use of PBZ digital banking for business entities (**hereinafter: General terms for digital banking**) shall regulate the rights, obligations, responsibilities and terms and conditions under which the Bank provides the service of PBZ digital banking (hereinafter: the Service) to business entities that have opened and hold a transaction account at the Bank.
2. The General terms for digital banking shall constitute an integral part of the Contract for the use of PBZ digital banking for business entities (**hereinafter: the Contract**).
3. The General terms for digital banking shall be considered to be separate general terms in relation to the General operating terms of Privredna banka Zagreb d.d. for transaction accounts and performance of payment services and other services for non-consumers (**hereinafter: General operating terms for transaction accounts**) and shall be applied together with the General operating terms for transaction accounts.
4. In the event of any conflict/discrepancy between the provisions of the Contract and the General operating terms for transaction accounts, the Contract shall be applied.
5. The Contract shall form an integral part of the Framework Contract, as defined and described in the General operating terms for transaction accounts, and in the event of any conflict/discrepancy between the provisions of this Contract and other documents constituting the Framework Contract, the Contract shall be applied.

2. DEFINITIONS

For the purposes of these General terms for PBZ digital banking, individual terms listed below shall have the following meaning:

#withSIGN - Qualified electronic signature – for the purposes of these General terms, a qualified electronic signature means a qualified electronic signature which is based on a qualified certificate issued to an End User, under a separate contract, by Intesa Sanpaolo S.p.A as a qualified trust service provider.

The Signatory shall use the issued qualified certificate to electronically sign the documentation when contracting the use of banking and financial service through this Service.

The signing of documents by using a qualified electronic signature shall be done in the following way: the Bank shall present a draft document to the Signatory in/via PBZ internet or mobile banking application of the Service and the Signatory shall be requested to enter an SMS code sent to a registered mobile phone number of the End User and certificate holder. Upon successful verification of the entered data, the document shall be considered electronically signed by means of a qualified electronic signature.

Administrative Attributes – are attributes that enable the End User who has been assigned the User role of a Master/Master admin to manage User rights, i.e. Transaction Attributes of other End Users who have been assigned the (user) role of an Operator. For the use of services integrated into the Service, administrative attributes are described in general terms for the use of those services.

Activation Code – a one-time password which is used together with the Identification Code for activation and personalisation of the PBZ mobile banking application;

Authentication – the process of identifying the End User through personalised security features. The authentication process allows the verification of the use of a particular Authentication/authorisation System, including the verification of personalised security features, thereby verifying the identity of the End User. If the authentication includes the use of two or more elements categorised as knowledge (something only the End User knows), possession (something only the End User possesses) and inherence (something the End User is) that are independent, it is considered strong authentication.

Authentication/authorisation systems – devices, applications or methods used for Authentication and authorisation for the purpose of enabling access to and use of the Service:

- **#withKEY** – an authentication and authorisation system integrated into the PBZ mobile banking app for the purposes of accessing and using the Service as well as making payment transactions initiated with a debit card for business entities on Internet points of sale. A PIN or one of the biometric methods (Touch ID, Face ID) are used for initiating this system.
- **Smart login** – a system of authentication and authorisation integrated into the PBZ mobile banking application for the purpose of enabling access to and use of the PBZ internet banking application of the Service, which uses sending of an automatic notification (Send push) or sending of the code in an SMS. An End User may, at his/her discretion, choose to use the Smart login system for authentication when accessing the Service. The Smart login system is also used for making TDS and payment transactions initiated with a debit card for business entities on Internet points of sale in the manner described in these General terms.
- **Biometric methods** – methods of authentication and authorisation that are based on physical characteristics of an End User (e.g. one's fingerprint, voice, face identification). The Bank, for the purpose of access to and use of the Service, may enable authentication and authorisation of an End User by applying biometric methods in accordance with the technical capabilities of the End User and the Bank. For the purpose of using biometric methods of authentication/authorisation for access to and use of the Service, the Bank may use [a piece of] personal data which the End User has stored with a third party (through the software on the device used to access the Service) and has activated it for authentication/authorisation within the Service (e.g. fingerprint i.e. touch



identification, face identification), without such data being stored by the Bank, or [the Bank may] collect, store and use biometric parameters of the End User subject to obtaining separate prior consent of the User.

- **Face ID** – a method of authentication and authorisation through recognition of the End User's face. The End User has previously, by taking an action that is independent of the Service, stored data containing the information on face identification by using the software on his/her mobile device that supports Face ID functionalities and, after that, he/she has activated such data in the PBZ mobile application in order to use the Service. Face identification is used by the End User to access the Service and/or to give consent for the execution of payment transactions. The End User may use biometric methods to the extent allowed by technological characteristics of the mobile device which he/she uses.
- **Touch ID** – a method of authentication and authorisation by using the End User's fingerprint which, as a piece of data, the End User has previously stored, by taking an action that is independent of the Service, using the software on his/her mobile device that supports a fingerprint reader and, after that, has activated such piece of data in the PBZ mobile banking application in order to use the Service. During the activation, the End User himself/herself shall, via the PBZ mobile banking application, define the scope of use of the touch ID in the context of the Service, and shall authorise all that has been mentioned above by entering the PIN which he/she has set as the PIN for using the PBZ mobile banking application. Fingerprint identification i.e. Touch ID is used by the End User to access the Service and/or to give consent for the execution of payment transactions on behalf and for the account of the User.

Authorisation – the procedure of confirming the will of the End User expressed on behalf and for the account of the User by using personalised security credentials and a particular Authentication/authorisation system, for the purpose of giving consent for the execution of payment orders, conclusion of certain contracts or for another purpose supported by the Service. By means of authorisation, the End User accepts, on behalf and for the account of the User, the terms and conditions presented to him/her before authorisation. The possibilities for and the way the authorisation is conducted depend on characteristics of the Service, and are defined in these General terms for digital banking and the Contract;

Bank – Privredna banka Zagreb d.d., Zagreb (City of Zagreb), Radnička cesta 50, Croatia (BIC/SWIFT: PBZGHR2X, account no. HR642340009100000013, TIN (OIB): 02535697732, e-mail: com@pbz.hr, website: www.pbz.hr) entered in the court register of the Commercial Court in Zagreb under the registration number: 080002817, the issuer of the General terms for PBZ digital banking for business entities;

Chat, video chat and audio chat communication - chat, video-chat and audio chat communication that the Bank can offer to End Users during their use of the Service through Internet and mobile application.

- **Chat** communication is a two-way written electronic communication between the End User and the Bank, it takes place in real time at the End User's initiative through the Service – Internet or mobile application, with the User's prior access thereto and authentication in the agreed manner.
- **Video chat** is a visual-voice communication between the End User and the Bank, it takes place in real time at the End User's initiative through the Internet or mobile application of the Service, with the User's prior access thereto and authentication in the agreed manner.
- **Audio chat** is a voice communication between the End User and the Bank, it takes place in real time at the End User's initiative through the Service – Internet or mobile application, with the User's prior access thereto and authentication in the agreed manner.

Electronic signature – data in electronic form which are attached to or logically associated with other data in electronic form and which are used by the signatory to sign;

Identification Code – a one-time password which is used together with the Activation Code for activation and personalisation of the PBZ mobile banking application;

Pre-login area of the Service – refers to the area of the Service, available to the public, as well as to the End Users of the Service, without having to log in to the application. It provides more information related to the Service functionalities, provides an overview of the Bank ATMs and branch offices/PBZ Sinergo desks as well as the Bank contact details. The End Users are additionally provided with the possibility to initiate the PBZ mobile banking login by using #withKEY authorisation device. The Bank reserves the right to change this publicly available content.

OTP - One Time Password – a series of numbers which is, on request, generated by means of #withKEY system, having a limited validity period, which is used for one-time identification of the End User for the purpose of enabling access to the Service and use of individual services offered by the Bank through the Service which require identification of the End User by means of an OTP, as well as for the purpose of authorisation of payment transactions and conclusion of certain contracts.

Recovery code – End user's personal secret identification number, known solely to the End User and strictly confidential, it serves for identifying the User in the reactivation process, i.e. application recovery process.

User rights – rights related to Transaction and Administrative Attributes, which (rights) can be granted to an End User who has been assigned a particular User role. The End User who has been assigned the Master role shall have all the rights (and Transaction and Administrative attributes), while a Master Admin[istrator] shall be granted rights related to Administrative Attributes, and the End User with given Operator rights shall be granted the rights with Transaction Attributes.

User ID – a unique identifier of the End User of the Service issued by the Bank when contracting the Service and used for the authentication and verification of the End User's identity required for their access and use of the Service. The End User shall be obliged to handle this data in line with item 6 of these General Terms.

User – a business entity that has opened and holds a transaction account at the Bank and has contracted and uses the Service referred to in these General terms for digital banking;



End User – an individual authorised by the User to use the Service, and other services available for use within the PBZ Digital banking for business entities, on behalf and for the account of the User, who - depending on the role he/she has been assigned - may be a Master or Master Admin[istrator] or an Operator;

Qualified electronic signature – is an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures. A qualified electronic signature shall have the legal effect equivalent to a handwritten signature;

Service Limit – the maximum amount of all transactions in euros and foreign currency which is placed at the disposal of the Service User in accordance with the rules defined in section 3 of these General terms.

Master – authorization by which an End User is assigned all Transaction and Administrative Attributes, i.e. all necessary authorisations to use the Service, which includes the right to contract the distribution of statements per business entity, the right to submit a request for issuance of BON-2 solvency information and the right to view the Payees. The Master may grant at the same time the User rights to all other End Users that have been assigned the role of an Operator, i.e. to the End Users who should be involved in the process of authorising Business transactions. The End User with assigned Master Role shall be enabled to use other services used within the Service as described in general terms for such services.

Master admin – the User role in which an End User has Administrative Attributes and may grant User rights to all other End Users that have been assigned the role of an Operator and may define groups of signatories, i.e. End Users who should be involved in the process of authorising Business transactions. The Master Admin role includes also the right of contracting the distribution of statements by/per a business entity.

Advanced electronic signature - is an electronic signature that is uniquely linked to the Signatory, is capable of identifying the Signatory, is created by using electronic signature creation data that the Signatory can, with a high level of confidence, use under his/her sole control and is linked to the data signed therewith in such a way that any subsequent change in the data is detectable;

Unusual transaction – is any payment which is made for the first time to an account not specified as a Trusted Account/Verified Payee.

Push Notifications – notifications which the Bank sends to an End User to his/her mobile device, using the phone number provided to the Bank by the End User, where the sending of such notifications has been previously selected and activated by the End User in the Service settings. The End User shall decide by himself/herself if he/she wishes to use i.e. activate sending of push notifications and shall, accordingly, select an option in the Service application, authorising this by entering a PIN or by using a Biometric method or by entering a one-time password, upon which this option shall be considered activated.

The Bank can notify the User with Notification(s) also within the scope of particular Service functionality used by a User/End User, which includes the sending of notices.

Operator – the User role in which an End User may have a combination of Transaction Attributes, to whom the Authorised Representative may grant User rights by means of a Request for granting user rights and/or to whom a Master/Master Admin may grant User rights related to particular business areas via PBZ digital banking applications. The User shall have the possibility to grant User rights for the Operator via applications of PBZ digital banking for business entities, without submitting a Request for granting user rights. The End User who has been assigned the role of an Operator has no Administrative Attributes. The End User with granted Operator role shall be enabled to use the services available within the Service, if he/she has been granted all required transaction attributes, defined in general terms for a particular service, and required for the user of the service.

Authorised Representative – an individual who represents the User by law or under a power of attorney, and who, on behalf and for the account of the User, grants authorisations i.e. assigns User roles to End Users in order to enable them to use the Service;

User role – a role assigned to every End User by means of the Request for the use of the Service. The roles of End Users may be those of a Master, Master Admin[istrator] and an Operator. Depending on the role assigned to an End User, it is possible to manage user rights of End Users.

Personalised Security Credentials – a unique number known only to the End User, and for the purpose of these General terms, they include the registration code (identification and activation codes) for the activation of the mobile app, the User ID, the PIN the End User has set for the mobile app and the #withKEY Authentication/authorisation system, the password for accessing the qualified electronic certificate (FINA Business Certificate), passwords generated by authentication systems/devices #withKEY and other credentials depending on the channel used and/or payment instrument.

PIN – a secret personal identification number of an End User, known exclusively to the End User and strictly confidential, which is used for identification of the User and the End User and authorisation in the case of transactions that require PIN identification and authorisation;

Payment instrument – any personalised instrument and/or a set of procedures agreed between the User and the Bank, which is used by the User for purposes of initiation, signing and authorisation of payment orders and all the other business transactions in the manner as defined by each business transaction; it can be, for example, #withKey.

Business transactions – all transactions whose execution is made possible by the Bank through the Service – payment transactions, treasury transactions, and all other transactions supported by the Service.

Business requests – all requests that can be made i.e. submitted by using the Service – requests for contracting [certain] services, requests for signing a contract for a time deposit, requests for financing and requests related to investment banking operations, as well as all other requests supported by the Service.

Business entity – a legal entity or an individual operating within the scope of his/her line of business or as a self-employed professional – non-consumer;

Business area – is an area covered by certain functionalities of the Service for which the End User may be granted User rights, such as euro payments from an account (euro debits), foreign currency payments from an account (FX debits), treasury operations and other Service functionalities to be subsequently introduced;



Signatory – the End User in possession of a Payment Instrument by means of which he/she signs and authorises payment orders on behalf and for the account of the User. A Signatory may have 50% of the signing authority when signing as one of the two authorised joint signatories, or he/she may have the full signing authority (100%) if acting as a single Signatory and may be granted signing authority for an individual Business area. This term also denotes the End User who creates the electronic signature based on qualified certificate for electronic signatures/ **#withSIGN – Qualified electronic signature**, issued to the End User under a separate agreement by Intesa Sanpaolo S.p.A as a qualified trust service provider, based on rights and authorisations granted to the Signatory by the User. The Signatory may place his/her signature electronically – independently/individually or jointly/co-signed (in pair) with another Signatory, for and on behalf of the User and/or on his/her own behalf and for his/her own account as the End User, as the case may be, and based on contracts concluded between the Bank and the User.

Payee – an account that the End User has entered/saved in the list of payees within the Service, which may or may not be designated as a Trusted Account/Verified Payee.

Post-login area of the Service – refers to the area of the Service which is accessible to the End Users of the Service after successful Authentication via an Authentication/authorisation system;

Trusted Account/Verified Payee – a functionality that enables credit transfer payment transactions to be credited through the Service, to an account of the payee that the User/End User has entered in the list of Payees and designated as a Verified Payee, and has designated his/her account as Trusted Account. In this connection, it shall be considered that the End User, for whom the process of Authentication has been previously conducted, after activation of the Trusted Account/Verified Payee functionality, has given consent for the execution of every initiated transaction, by Authorisation with the use of #withKey code, which is to be credited to an account that has been added to the list of Payees and designated as Trusted Account, and his/her holder as Verified Payee. The End User, for and on behalf of the User, shall decide by himself/herself if he/she wishes to use the possibility of designating (marking) the payee as verified/trusted, and shall, accordingly, authorise this action in the application, upon which this functionality shall be considered activated. It is not required to authorise deactivation of this functionality.

Registration Code – a one-time password which consists of an Identification Code and an Activation Code.

Means of distance communication – include means which, without the simultaneous physical presence of the End User and the Bank, may be used for access to and use of the Service, including also remote conclusion of contracts: the PBZ internet banking application, the PBZ mobile banking application, telephone connection and other means to be subsequently introduced by the Bank.

TDS (Transaction Data Signing) payment transaction – a transaction directed to a payee's account that has not been entered by the End User in the list of payees and designated as a Trusted Account/Verified Payee Account. The End User shall grant consent for the execution of TDS transactions by entering, on the authorisation interface, the authentication code generated and relative to the payment transaction amount and the payee, indicated by the payer when initiating the transaction through some of the authentication/authorisation systems: Smart login (by sending an automatic #withKey (scanning QR code)).

Transaction Attributes – are User rights which the User and/or a Master/Master admin grants to an End User having the role of an Operator in relation to an individual business area and in relation to a particular transaction account or all transaction accounts of the User. Transaction attributes granted to End Users having the Operator role for the use of services integrated in the Service are described in the terms for such services.

Transaction attributes include the following rights:

- View* – the End User shall be able to view orders, transactions, order templates, requests and other information related to an individual business area for which he/she has been granted the User right; enables the use of account information service and payment initiation service; within the scope of the service #withMYBANKS, to the End User, who has been granted the attribute of designated account view, the transaction attributes of entry and authorisation shall be automatically granted in 100%;
- Upload* – the End User shall be able to upload orders and requests by entering data or by uploading files, and he/she can amend or delete the orders and requests entered by End Users;
- Authorisation* – the End User shall be able to sign and authorise orders/requests and send them for execution. The End User who has been granted the full authorisation right (100%) shall be entitled to act as a single signatory and authorise orders/request independently, so that any order that has been authorised 100% shall be considered signed/authorised and can be sent for execution. In the case of signing/authorisation by two joint signatories, each End User who has been granted 50% of the right should sign and authorise an order, so that the order shall be considered signed/authorised after having been signed/authorised by both End Users. The order that has not been signed/authorised 100% shall be regarded as not signed/authorised and cannot be sent for execution. Any End User who has the authorisation right of 50% or 100% shall be able to set a daily limit for authorisation in respect of User rights related to an account, and the amount of the daily limit for authorisation may be lower than or equal to the Service Limit;
- Report* – the End User shall be able to view statements and invoices related to transaction accounts as well as contractual documentation and to submit requests for issuance of BON-2 solvency information; To submit a request for issuance of BON-2 solvency information, it is necessary that the End User has at least been granted the report User right for the payment - euro debits business area. If the End User has been granted the report User right for the payment - euro debits area, then s/he can submit a request for issuance of BON-2 solvency information for the euro component of one or all transaction account(s) of the User. If the End User has been granted the report User right for the payment - euro



debits and FX debits areas, then s/he can submit a request for issuance of BON-2 solvency information for the euro component or all components (currencies) including the euro of one or all transaction account(s) of the User. If the End User has been granted the report right only for the payment - FX debits area, then s/he cannot submit a request for issuance of BON-2 solvency information.

Contract – enables the End User to contract services for business areas available within the scope of the Service (for example cards, financing, term depositing).

Contract for the use of PBZ digital banking for business entities – the document based on which the Service is contracted;

#withMYBANKS service for business entities – a service which is integrated and used within the PBZ Digital banking service for business entities. It comprises two payment services: payment initiation service and account information service through which it enables the User, via a legal representative and/or end users with granted Master operator or Operator roles, with Internet access through remote communication channels, to designate (connect) one or more transaction accounts open with other payment system service provider(s) holding the accounts of the same User, to view the balance and/or movement(s) (transaction list) of designated (connected) accounts, to initiate transactions debiting the designated accounts.

The service of PBZ digital banking (the Service) – enables a Client, through an Authorised representative and/or appointed End Users, to accept and use banking and financial services, through remote communication channels, to view the account balance and list of transactions in accounts, to accept the certification services and to conclude specific contracts related to the provision of banking and financial service in electronic form. The Service also makes it possible for the User to view information on the services offered by the Bank, through the Authorised representative and/or appointed End Users, on its own behalf and for its own account or for the account of third parties on the basis of contracts entered into by the User and pursuant to regulations. The use of the Service shall depend on the offer of the Bank, the currently valid regulations and the manner of using the Service.

Request for the use of PBZ digital banking for business entities (hereinafter: the Request for the use of the Service) – forms an integral part of the Contract and, by means of this document, the User grants authorisations [i.e. assigns User roles] to End Users related to the use of the Service and assigns and/or revokes basic authorisations [i.e. User roles] granted to End Users that enable access to and use of internet and/or mobile PBZ digital banking on behalf and for the account of the User; further, by means of this document, the User specifies/changes the mobile phone number and the e-mail address of the User/End User, defines the accounts for calculation and collection of the monthly fee for the Service. By means of the Request for the use of the Service, the User may request a change of the Service Limit and of the PBZ mobile banking application limit. If the requested amount of the Service Limit and/or the PBZ mobile banking application limit exceeds the amount of the limit initially set by the Bank, the User should fill in the additional form entitled Statement and request for a change of the daily limit for PBZ digital banking for business entities.

The User may submit the Request for the use of the Service several times for the duration of the Contract, and, after each new submission of this Request, the most recent Request shall be considered relevant in terms of providing the necessary information, as a supplement to the previous Request for the use of the Service (the Service cannot be cancelled by submitting a new Request for the use of the Service; it can be cancelled only in the manner stipulated in Article 7 of the Contract).

Request for granting user rights for PBZ digital banking for business entities (hereinafter: the Request for granting user rights) – forms an integral part of the Contract and, by means of this document, the User assigns to an End User, having the Operator role, the User Rights/Transaction Attributes related to individual business areas and transaction accounts of the User.

The User may, on more occasions during the Contract validity period, change the assigned User rights, and specifically with each new change via the PBZ Internet banking application or with each new submission of the Request for granting user rights. Concerning the entered data, the most recently made change shall be deemed applicable as a supplement to the previously submitted Request for granting user rights.

Statement and request for a change of the daily limit for PBZ digital banking for business entities (hereinafter: the Request for change of daily limit) – the document on the basis of which the User requests an increase in the daily Service Limit and/or the PBZ mobile banking application limit set by the Bank.

3. CONTRACTING OF THE SERVICE

1. A precondition for contracting the service is a transaction account that has been opened at the Bank.
2. The User shall be obliged to deliver to the Bank the correctly filled-in and signed Contract together with the Request for the use of the Service, on the basis of which the Service is contracted, on paper or in electronic form, if the Bank offers the possibility to conclude a contract for the Service in electronic form.
3. When the Service is contracted, the User's Authorised representative shall grant authorisations to one or more End Users allowing them to use the Service on behalf and for the account of the User. On that occasion, the User's Authorised representative shall decide if the relevant End User shall have the User role of a Master, Master admin or an Operator. If the End User is to be assigned the role of an Operator, the User's Authorised representative shall be required to fill in the additional form, the Request for granting user rights.

Any Master and Master admin shall be authorised to grant, revoke and change, via the PBZ internet and/or PBZ mobile banking application, authorisations [i.e. user rights] granted to other End Users having the role of an Operator. The User may request, on the basis of the signed Request for the use of the Service, that a Bank employee, acting on behalf and for the account of the User, on the basis of the filled-in Request for the use of the Service signed by the User, grants,



revokes or changes authorisations i.e. information related to other End Users in the PBZ digital banking application. The User shall have sole liability for the information stated in the Request for the use of the Service, based on which the Bank employee will enter data in the system, at the request of the User.

4. A change of authorisations granted to End Users may be made:

- a) directly by the User and/or the End User having the role of a Master or Master admin, via the PBZ internet and/or PBZ mobile banking application;
- b) indirectly by the User, with the assistance of a Bank employee, based on the Request for the use of the Service which must be filled-in and verified by the User.

The Bank defines two types of daily limit at the Service level, which are the Service Limit and the PBZ mobile banking application limit. The Service Limit represents the total amount that is at the User's disposal in both applications - the PBZ mobile banking application and the PBZ internet banking application, which may be larger than or equal to the PBZ mobile banking application limit. The PBZ mobile banking application limit represents the total amount that is at the User's disposal in the PBZ mobile banking application. The Bank shall be entitled to set at its own discretion, without having to provide any explanation, a daily limit for the use of funds in relation to a particular transaction account of the User and/or in relation to a particular End User and/or in relation to the Service and/or the PBZ mobile banking application. The amount of the limit that has been set in this way shall be visible in the PBZ internet and/or PBZ mobile banking application. The amount of the approved limit may be changed, and it may be subsequently decreased or increased in accordance with a written request of the User, or within the application. A change of the limit up to the amount which the Bank has set as a pre-defined limit may be requested by submitting a Request for the use of the Service, or may be changed by the Master user in the Service applications, while for an increase in the limit exceeding the pre-defined limit amount it shall be necessary to fill in the Statement and request for a change of the daily limit of the Service. If the User has not requested any change of the daily limit up to the maximum limit set by the Bank, then the limit defined by the Bank shall be the applicable limit. If a daily limit for the use of funds via this Service has been set, the User and End Users shall be allowed to use the Service only up to the amount of the set daily Service Limit and/or the PBZ mobile banking application limit. By signing the Contract, the User accepts and agrees that the Bank shall have the right to set, change and abolish the daily limit for the use of funds referred to in this section at its own discretion.

Daily limit for the disposal of funds shall be reduced as described in more detail in the User instruction for PBZ Digital banking service for business entities. If a payment order has no order execution date entered before the Pay action, then after the Pay action the date on which the Pay action was performed shall be assigned in the Service as the order execution date. If a payment order has the execution date entered before the Pay action, then the Pay action shall reduce a daily limit for the disposal of funds in the amount of the order for the execution date entered.

3.1. Contracting of the Service at PBZ Sinergo desk

1. The User may contract the Service at a PBZ Sinergo desk, by signing the Contract and the Request for the use of the Service, and, optionally, also the Request for granting user rights if the relevant End User is to be assigned the role of an Operator.
2. When contracting the Service, the User shall download the PBZ mobile banking application and, after starting the application, should enter the Registration Code. The Bank shall send the Registration Code needed for activation: the Identification Code shall be delivered in an SMS message sent to the mobile phone number which the User/End User provided when contracting the Service, and the Activation Code shall be delivered [to the User/End User] at the Sinergo desk of the Bank.
3. The Bank reserves the right to refuse to sign the Contract and the Request for the use of the Service if the User and/or the End User refuse(s) to provide data which are necessary for the performance of the Contract and for carrying out activities prior to entering into the mentioned Contract and/or if any of them refuses to provide data which are necessary for the fulfilment of legal obligations of the controller or the exercise of the official authority of the Bank as the controller.
4. The Bank reserves the right to refuse to sign, for any reason, the Contract and the Request for the use of the Service and it shall not be obliged to provide any specific explanation for the refusal.

3.2 Contracting the Service via PBZCOM@NET electronic banking services

1. The User of the existing PBZCOM@NET electronic banking service may contract the Service via PBZCOM@NET electronic banking service, where the authorised representative of the User in their capacity as the End User shall access the PBZCOM@NET service, whereby the User shall contract the new Service online by providing existing personalised security credentials generated by PBZmToken or PBZ smart card or PBZ USB device for accessing and using the PBZCOM@NET electronic banking service and by signing documentation with an advanced electronic signature (confirmed by FINA (Financial Agency) business certificate) or an authorization with a One-time password OTP. Upon contracting the new Service, the User may activate the PBZ mobile banking app as part of the electronic banking service. Upon the successful activation of the PBZ mobile banking, the PBZ internet banking app is available for use to the User.
2. The End User shall download the PBZ mobile banking app, and the Bank shall send to the End User the Registration Code required for activation: the Identification Code shall be sent via SMS to the mobile phone number which the User/End User provided to the Bank for that purpose, and the End User shall download the Activation Code in the document that is



available upon successful completion of the process of contracting Digital Banking for business entities via PBZCOM@NET electronic banking. The Bank may make available part of the Registration Code in the PBZ internet banking app.

3. After the service has been contracted, the executed orders, rejected orders and order templates shall be transferred from the PBZCOM@NET electronic banking service.

4. The User who contracts the Service via PBZCOM@NET electronic banking shall be able to contract the Service on the basis of predefined data verified by the Bank. The User who meets all the criteria shall receive a notification about the possibility of contracting the new Service, together with the link to be used for this purpose.

4. TERMS AND CONDITIONS FOR USE OF THE SERVICE

1. A Contract for the use of the Service may be concluded at a PBZ Sinergo desk and/or on the web portal of the Bank. To make the use of the Service possible, the Bank uses technological solutions that ensure a connection between the User's equipment and the Bank's computers which meets the standard security conditions for *online* banking. In order to be able to use the Service via the PBZ internet banking application, the User shall be required to ensure access to the Service and connection to the internet from a desktop or laptop computer, a tablet or other device which is used for access to the Service. In order to be able to use the PBZ mobile banking application, the User shall be required to have a mobile device i.e. a mobile phone with adequate technical characteristics.

2. In order to prevent any unauthorised access and fraud in connection with the use of the Service, since this Service refers to the use of *remote* banking and financial services, the Bank may, by using specialised software tools, analyse the features of the way in which an End User uses the service (for example, dwell time on certain data entry fields, navigation between entry fields using the mouse, keyboard or fingers, as well as combining this with technical data that represent preconditions for being able to use the Service through means of distance communication, for example, the operating system which the End User uses, the type of mobile device/computer, the type and version of the browser – with regard to web applications, the size of the screen of the device, the language of the browser/mobile device, the name and version of the mobile application, and, if necessary, other data of this kind).

3. When contracting the Service, the User/End User shall be obliged to provide to the Bank the mobile phone number to which the Bank should send the Registration Code (Identification Code) needed for activation of the PBZ mobile banking application. On the same mobile device, one End User can use the Service for multiple different Users.

Depending on the stipulations of the Decision of the Bank and the currently valid regulations, it may be possible to contract certain services that are offered via the Service only by using a valid qualified certificate, by signing the documents by means of a qualified electronic signature.

4.1. Access to and use of the Service via the PBZ mobile banking application

1. The User shall be able to use the Service every day, on a 24-hour basis, via the PBZ mobile banking application installed on a mobile device of an End User. In order to be able to access and use the Service via the PBZ mobile banking application, the User shall be required to have a mobile device with adequate technical characteristics (a smartphone or other mobile device using the adequate operating system and the adequate version of the operating system). The End User may download the PBZ mobile banking application from App Store or Google Play Store, depending on the mobile platform which he/she uses.

2. The Service may be accessed via the PBZ mobile banking application only by using #withKEY authentication/authorisation system. The PBZ mobile banking application may be activated after contracting the Service at a PBZ Sinergo desk and/or on the web portal of the Bank. Upon contracting the Service at a PBZ Sinergo desk, the End User shall download the PBZ mobile banking application and install it on his/her mobile device, and the Bank shall send to the End User the Registration Code needed for activation of the PBZ mobile banking application: the Identification Code shall be delivered in an SMS message sent to the mobile phone number which the User/End User provided to the Bank to be used for that purpose, and the Activation Code shall be delivered [to the End User] at the PBZ Sinergo desk or through another distribution channel.

3. After the mobile application has been installed and activated by entering the one-time Registration Code assigned to the End User by the Bank, the next step is defining of personalised security credentials – a PIN, which is to be created by the End User himself/herself for the purpose of access to and use of the PBZ mobile banking application. The PIN shall be used by the End User for the purpose of Authentication when logging in to the Service, for giving consent for the execution of payment transactions on behalf and for the account of the User, for concluding contracts if the End User is at the same time the Authorised Representative [of the User], or for any other purpose which is offered via and supported by the Service, in accordance with the currently valid regulations. The End User may, for the purpose of access to and use of the Service via the PBZ mobile banking application, depending on his/her needs and capabilities, apart from the PIN, also use a biometric method. The User agrees to the End User's choice of the Authentication/authorisation system to be used by the End User for the purpose of authentication and/or authorisation in the PBZ mobile banking application.

4. When the Service is accessed and used via a PIN, Authentication of the End User shall be conducted when logging in to the Service as well as when giving consent for the execution of payment transactions (authorisation of transactions) and giving other types of consent and making other declarations of will in the context of the Service, in such a way that the End User should enter a PIN which is to be used for this purpose in the proper field on the screen of the mobile application. If the End User has opted for the use of a PIN when giving consent for the execution of payment transactions and giving other types of consent or making other declarations of will, it is not necessary to authorise such transactions by means of a Biometric method. When the Service is accessed and used via Touch ID, Authentication of the End User shall be conducted when logging in to the Service and/or when giving consent for the execution of payment transactions (authorisation of transactions), in such a way that the End User should press a finger on the relevant spot on the screen of the mobile application. If the End User has chosen to use Touch ID for giving consent for the execution of payment transactions, it is not necessary to authorise them by means of a PIN. In the PBZ mobile banking application the End User



may choose whether he/she will use Touch ID only for logging in to the Service or for [both] logging in to the Service and giving consent for the execution of payment transactions. When the Service is accessed and used via Face ID, Authentication of the End User shall be conducted when logging in to the Service and/or when giving consent for the execution of payment transactions (authorisation of transactions), in such a way that the End User should, at the proper moment, use Face ID. If the End User has chosen to use Face ID for giving consent for the execution of payment transactions, it is not necessary to authorise these transactions by using other Biometric method or a PIN. In the PBZ mobile banking application the End User may choose whether he/she will use Face ID only for logging in to the Service or for [both] logging in to the Service and giving consent for the execution of payment transactions.

5. If the installed PBZ mobile banking application is locked, deleted, or if the End User wishes to install the application on another mobile device and not on the one currently used, it shall be necessary to obtain a new Registration Code (Identification Code and Activation Code) in order to re-activate it. The End User of the Service may request the issuance of a new registration code for activation of the PBZ mobile banking application at a PBZ Sinergo desk or via another distribution channel, of which the Bank shall notify the End User. The End User may request the Service Recovery Code by submitting a request exclusively to the Bank.

The User/End User of the Service shall be obliged to provide to the Bank a correct mobile phone number to which the Bank shall then send a new Identification Code via an SMS message. If the End User of the Service has requested a Registration Code, and it turns out that the mobile phone number which the User/End User of the Service has provided to the Bank is no longer active or if the User/End User of the Service has not provided to the Bank any mobile phone number as a piece of contact information, the Bank shall not be liable for any damage that may be suffered by the User due to non-delivery of the Registration Code (Identification Code) or in the event of delivery of the registration code (Identification Code) to the most recent mobile phone number which the User/End User of the Service has provided to the Bank as a piece of contact information.

6. The content, scope and the manner of using the Service via the PBZ mobile banking application are described in more detail in the User instructions available on the website of the Bank, on the screen of the mobile application as well as at a PBZ Sinergo desk.

4.2. Access to and use of the Service via the PBZ internet banking application

1. The User shall be able to use the Service via the PBZ internet banking application every day, on a 24-hour basis, by using the Authentication/authorisation systems of End Users. In order to be able to access and use the Service via the PBZ internet banking application, the End User should go to the web address www.pbz.hr, on the menu Registration/Login in the segment referring to business entities. In order to be able to access and use the Service via the PBZ internet banking application, the User shall be required to ensure connection to the internet from a desktop or laptop computer, a tablet, or other device which is used for access to the Service.

For access to and use of the *On-line* banking via the Internet application, the Bank makes it possible for the User to use the #withKey authentication system implemented in the PBZ mobile banking application, and can also provide the authentication card reader, token or PBZmToken to the user.

2. Access to and use of the Service via the PBZ internet banking application shall be enabled upon using one of the Authentication/authorisation systems listed below:

- **#withKEY**- the End User should access the www.pbz.hr page and authenticate himself/herself under the segment Login by entering the User ID number shown on the screen of #withKEY system of the PBZ mobile banking application and by entering a one-time password (#withKey code) generated by #withKEY system in the "One time password" field.
Authorisation of transactions and giving of consent and making of declarations of will shall be conducted in two ways:
- **Authorisation by scanning of the QR code (TDS payment transactions)** – used when authorising payment transactions in such a way that the QR code is shown on the PBZ Internet banking screen, which contains elements of one or more payment orders, specifically: payee's name, payee's account number, transaction amount and execution date. The End User can choose the option „Scan the QR code“ in the segment of the #withKEY authorisation system by way of which he/she scans the QR code and the order elements appear on the screen. Having checked the accuracy of the shown data, the End User authorises the payment transaction(s) by entering the PIN defined for the use of the PBZ mobile banking or by using the biometric method, whereby the payment transaction is considered authorised.
- **Authorisation with one-time password** – used for the authorisation of payment transactions with Trusted Account/Verified Payee, for giving consents and other transactions by entering, in the proper field on the screen, a one-time password generated by the #withKEY authorisation system.
- **Smart login (Smart authorisation)** – Access to the Service in the PBZ internet banking application shall be enabled in the following way: the End User shall choose, on the appropriate spot on the web page www.pbz.hr in the segment Login, the sending of an automatic notification (Send push) and cell phone number delivered by the End User to the Bank and used for the Service. After receipt of automatic notification, the End User shall enter a PIN in the PBZ mobile banking application or shall use a Biometric method, upon which access to the PBZ internet banking application shall be considered authenticated.

The procedure of payment order authorisation within the Service is completed in such a way that the application sends an automatic notification to a cell phone number which the End User has previously provided to the Bank and uses it in the context of the Service. Upon receipt of a notification which contains elements of a payment order, namely: the transaction amount, the execution date of the payment order, the account of the payee and the name of the payee, the End User shall authorise the payment transaction by entering a PIN or by using a Biometric method in the PBZ mobile banking application, upon which the transaction shall be considered authorised.



3. Authorisation shall be conducted by entering in the proper field in the PBZ internet banking application a one-time password generated by a token. Individual TDS transactions, which are authorised by means of SMS authorisation, represent an exception to this procedure.
4. The content, scope and the manner of using the Service via the PBZ internet banking application are described in more detail in the User instructions for the Service available to the Users/End Users on the website of the Bank (www.pbz.hr).
5. The User agrees to the End User's choice of the Authentication/authorisation system to be used by the End User in the PBZ internet banking application for the purpose of authentication and/or authorisation.

4.3. Use of services within the Service

4.3.1. #withMYBANKS Service for business entities

The #withMYBANKS Service can be contracted at a Sinergo desk or using the PBZ Digital banking service for business entities as described in the General Terms for the #withMYBANKS service. The #withMYBANKS service is used within the Service and encompasses the account information and payment initiation services.

Once the User's authorised person has contracted the #withMYBANKS service, it becomes available for use to all End Users of the Service who have been assigned transaction and administrative attributes defined as preconditions for the use of services incorporated in the #withMYBANKS service for business entities.

The account information service through consents enables the determining/identifying (connecting) of active accounts, available on-line, of other payment system providers holding the User's accounts, to the PBZ Digital banking service. The consent can be initiated by the End User of the #withMYBANKS service who is also the End User of this Service, with assigned Master role and the End User with given Operator role with assigned transaction attribute for viewing at least one transaction account open with the Bank within the scope of the Service. When initiating the consent, the End User selects the accounts he/she wishes to connect and chooses whether he/she wishes to view (have insight into) the balance and/or movements in selected accounts in the #withMYBANKS service. The consent for determining/identifying (linking) the accounts shall be authorised with a credential presented by another payment system provider where the selected accounts are open.

User rights for determined (linked) accounts are assigned in the Service Setups. The End User with Master role has the right to view all determined/identified accounts and assigns the transaction attribute for viewing to end users Operators. Transaction attributes of upload and autonomous order authorisation are automatically assigned to all End Users with assigned transaction view attribute.

Payment initiation service allows the initiation of payment debiting the determined (linked) accounts. Payment debiting the determined (linked) account may be initiated by End Users with assigned Master role and End Users with assigned Operator role, provided that the transaction view attribute of the determined account is assigned, which is debited within the payment initiation service. The payment debiting the determined account is authorised with a credential given by the payment system provider where the determined account is open, in accordance with the terms and conditions from the framework contract concluded between the User and the payment system provider holding the account.

The terms for the use of the #withMYBANKS service for business entities within the Service are described in the General Terms for the #withMYBANKS service for business entities, which are applied jointly with these General Terms for the use of the PBZ digital banking for business entities.

4.3.2. Card operations / Debit cards for business entities

The PIN for the debit card for business entities is available in the mobile application of the Service if the Service has been contracted and if the End User has authorization for card operations, has the technical prerequisites for displaying the PIN on the mobile device and if the End User of the Service is also the card user. The End User of the Service, who is also the card user, can activate the inactive debit card for business entities via the PBZ mobile banking application and the PBZ internet banking application.

5. SCOPE OF THE SERVICE

1. Information about the offered Service is available throughout the business network and on the website of the Bank (www.pbz.hr).
2. Regarding the contracted Service, the Bank shall make it possible for the User to use the Service in accordance with the scope of the Service and in such a manner as stipulated in the User instruction for the Service.
3. The Bank reserves the right to change the type, scope and content of the Service. Any change of the type, scope and content and/or introduction of new services shall be posted on the website of the Bank (www.pbz.hr). The User shall not be entitled to claim compensation for damage in the case of changes of the scope and content of the Service.



By signing the Contract, the User agrees to such changes and fully accepts them, and the Bank may consider that the User has been informed of and accepts the said changes if, within 15 days from the date when the changes were posted on the website of the Bank, the User does not cancel the Contract.

4. The User shall be entitled to use the Service in the manner provided for in the Framework contract, the User instruction for the Service and the User instructions for the areas within the Service posted on the website of the Bank or available in writing throughout the business network of the Bank. The Bank shall be authorised to amend the said User instructions and any such amendment shall be posted on the website of the Bank (www.pbz.hr). By signing the Contract, the User agrees to and fully accepts such amendments to the instructions.

6. USER'S OBLIGATIONS

1. The User/End User undertakes:

- for the purpose of use of PBZ digital banking and other services within the Service, to obtain, use and maintain adequate computer equipment (hardware and software) and communications equipment which meets the criteria for the Service use and which conforms to the recommended configuration posted on the website of the Bank, on which an adequate operating system, web browser, antivirus protection and a firewall should be installed and kept updated, in accordance with all the latest available producer updates;
- to protect the computer equipment and the application software for the use of PBZ digital banking and other services within the Service, and to use it exclusively in such a manner as is stipulated in connection with the Service use;
- to safeguard the devices and data used for authentication and authorisation in such a way to prevent their damage, destruction, loss, unavailability, theft or misuse;
- to safeguard carefully Payment Instruments, the User's own devices that enable access to the Service and other services within the Service, such as computers, mobile devices, etc., in order to prevent their loss, theft or misuse;
- to use any Authentication/authorisation system in such a way to preserve its confidentiality: a password, PIN as well as data generated by the relevant Authentication/authorisation system must not be written down, disclosed nor made accessible to third parties;
- to safeguard carefully user names, passwords, codes, PINs and other identifiers, to protect them from theft, loss, damage, destruction or misuse; as well as not to write them down on paper, in electronic form or by using other media; nor to disclose them nor make them accessible to third parties;
- to carry out all activities that are carried out via this Service in conformity with the Framework Contract and general terms regulating the use of individual service within the scope of the Service, as well as with laws and other regulations;
- to regularly check notifications sent by the Bank.

2. The User shall be required:

- to notify the Bank without delay of any loss, theft or misuse of an Authentication/authorisation device, a Payment Instrument on which the PBZ digital banking application has been installed, or of its unauthorised use, and the Bank shall, upon receipt of such notification, block the Authentication/authorisation device and/or the Service. Any successful access to the Service, any authentication and authorisation recorded before notifying the Bank, shall be regarded as having been carried out by the User.
- to promptly notify the Bank of any detected irregularities or unusual occurrences when using the Service;
- to notify the Bank of any change in personal information necessary for smooth and secure use of the Service, for example, any change in mobile phone numbers or e-mail addresses through which the Service is used. If the User fails to do so, the Bank shall regard the most recent data provided to the Bank by the User as relevant data and (the Bank) cannot be held liable for any damage caused by data not being up to date;
- to notify the Bank of a change in any data on the User entered in the relevant register (e.g. the name of the business entity, TIN (OIB), authorised representatives, etc.);
- to notify the Bank of a change in any End User's personal data (e.g. his/ her first and last name, TIN (OIB), address and place of residence, e-mail address, etc.);
- to notify the Bank of a change in the e-mail address and the mobile phone number of the User/End Users by submitting a new Request for the use of the Service. If the User does not change the above-mentioned data in this way, it shall be considered that the User has not requested a change of the above-mentioned data, and the Bank shall regard the most recent data provided to the Bank by the User in/via the previously submitted Request for the use of the Service as relevant data and (the Bank) cannot be held liable for any damage caused by data not being up-to-date;
- notify the Bank in person of revocation of authorisations granted to i.e. User roles assigned to any of the End Users.



7. BANK'S OBLIGATIONS

1. The Bank shall provide the User with all elements necessary for enabling access to and use of the Service during business hours that apply to a particular service, except in cases of force majeure, technical difficulties or other unexpected events.
2. The Bank shall continuously work on the development and improvement of the Service and, at the same time, shall be obliged to make the Service available to the Users on a regular basis and fully functional.
3. The Bank shall notify the Users in advance of any planned Service maintenance activities, which may result in the Service being temporary unavailable, i.e. in the Users being partly or fully unable to use the Service.
4. Regular Service maintenance shall be carried out at such times when the Bank expects that the Service is most likely to be used by the smallest number of users.
5. In the event of any unforeseen unavailability, the Bank shall take measures to eliminate the difficulties as soon as possible.
6. The Bank shall not be liable for any damage the User may suffer as a result of:
 - non-functioning or malfunctioning of computers, mobile or other devices which are not owned by the Bank, but which are used for access to the Service;
 - non-functioning of the computer system or the operating system of mobile devices used for access to the Service;
 - tampering by the End User or by another unauthorised person with the assigned device and/or with the application for Authentication/authorisation;
 - actions or omissions by a legal entity that provides mobile and/or fixed telecommunications services to the User and/or the Bank;
 - force majeure events, which include war, riots, terrorist acts, natural and environmental disasters, epidemics, strikes, power failures, failure of telecommunication lines and of other communication lines, errors in data transmission via telecommunication networks, decisions and actions taken by the authorities, as well as any other similar circumstances whose occurrence cannot be attributed to the Bank or which are beyond control of the Bank, and which make impossible access to the Service;
 - any loss, damage or destruction of data and equipment used by the User for access to the Service.
7. The Bank shall not be liable for any damage caused by the inability to provide the Service for reasons provided for in the General operating terms for transaction accounts.
8. The Bank shall not be liable for any damage caused by unjustified actions of the User or third parties, resulting in malfunctioning of the Service.
9. The Bank shall be liable to the User for any direct damage caused intentionally or as a result of negligence on the part of the Bank.
10. The Bank shall notify the User in the case of any suspected or actual fraud or a threat to the security of the Service and/or a Payment Instrument, using the available trusted channels and method of communication.
11. The Bank reserves the right to block further use of the Service by the User via the PBZ mobile banking application if an End User has not installed on his/her mobile device the current version of the PBZ mobile banking application, if an End User has in any way modified the operating system originally installed by the manufacturer (and/or the User rights) or its official upgrade (and/or the User rights) on the mobile device on which the PBZ mobile banking application has been installed. In the mentioned cases, it will no longer be possible to start the PBZ mobile banking application even after the mobile application has been reactivated by means of a new registration code, so that the use of the application shall be permanently blocked on that particular mobile device.

8. EXECUTION OF PAYMENT TRANSACTIONS

1. The Bank shall execute payment orders which are correctly issued via the Service in conformity with the time schedule specified in the document "Time of receipt and execution of payment orders/Cut-off time" currently in force, which forms an integral part of the Framework Contract.
2. The system shall notify the End User of receipt of a payment order which is issued/submitted for execution via the Service by means of a message about a successfully received payment order. Receipt of a payment order does not necessarily mean that the order will be executed, it only means that it has been received for execution. Execution of payment orders is regulated by the General operating terms for transaction accounts.
3. A payment order submitted/issued via the Service that enables issuing of payment orders shall be deemed to be electronically signed, authorised by and issued on behalf and for the account of the User. The End User to whom the User has granted the signing authority for a particular business area shall, on behalf and for the account of the User, give consent for [the execution of] a payment order by using the Authentication/authorisation systems in accordance with Article 4 of these General terms.
4. A payment order issued via the Service, but only an order with a future execution date, can be revoked via the Service, if the User wishes to do so, before the cut-off time for receipt of orders on a business day which precedes the business day in the course of which the order is to be executed in the manner provided for in the User instruction for the Service through which an order may be issued and revoked, which instruction is posted on the website of the Bank (www.pbz.hr).



5. The Bank shall not be liable for non-execution or late execution of an authorised payment transaction or defective execution of payment transactions or execution of unauthorised payment transactions in the following cases:

- if the execution of an unauthorised transaction and/or late execution of an authorised payment transaction and/or non-execution and/or defective execution of a payment transaction are the consequence of fraud committed by the User, fraud committed by the User's authorised persons/End Users, or if the User or the User's authorised person/End User does not meet the obligations set out in these General terms for digital banking and/or General operating terms for transaction accounts which regulate the handling of Payment Instruments in connection with taking of measures to protect personalised features of a Payment Instrument;
- if it is established that the User's payment order has been forged;
- in respect of the segment for which the User is liable pursuant to Article 10 of these General terms for digital banking, if the execution of an unauthorised payment transaction is the consequence of the use of a stolen or lost Payment Instrument or a misused Payment Instrument;
- if the execution of an unauthorised transaction and/or late execution and/or late execution of an authorised payment transaction and/or non-execution and/or defective execution of a payment transaction are the result of exceptional and unforeseeable circumstances which are beyond control of the Bank and which the Bank, despite its best efforts, is unable to influence and where the consequences of such circumstances would be unavoidable;
- if the obligation of execution of a payment transaction is based on the law or another regulation that is binding on the Bank.

6. The User shall be liable for, and shall bear the damage caused by, unauthorised payment transactions executed by using a Payment Instrument, regardless of the amount of a payment transaction, which (unauthorised transactions) are the consequence of a Payment Instrument being lost or stolen, or the consequence of other misuse of a Payment Instrument, up until the moment when the loss or theft or unauthorised use of a Payment Instrument is reported to the Bank. The User as the payer shall be liable for the executed unauthorised payment transactions if they are the consequence of the User's fraudulent actions or the User's intentional failure to meet one or more obligations under the Framework Contract concerning the manner in which a Payment Instrument is used or the manner in which personalised security credentials are handled or the failure to meet the said obligations due to gross negligence.

7. The Bank shall notify the User of all changes in the transaction account, including those made via the Service, by means of an account statement to be sent to the User in accordance with the instructions given in the Request for opening and managing a transaction account, which is an integral part of the Framework Contract as regulated by the General operating terms for transaction accounts. In the case of such alterations, the Bank shall regard as valid the most recent instructions given via the PBZ digital banking service, to which the User shall give consent and agree by signing the Contract.

9. SECURITY

1. The User shall be obliged to comply with all security measures and protection measures related to the use of computers, mobile devices and other devices on which the use of the Service has been activated in accordance with the security recommendations of the Bank, including:

- protection of access to a computer, to mobile and other devices by using a secret password;
- protection of secrecy of the selected password/PIN in order to prevent unauthorised use;
- not opening e-mail messages nor attachments and links included in suspicious e-mails or e-mails whose receipt is not expected;
- paying attention to websites which [the User/End User] visits using the same device from which the Service is accessed, since visits to certain websites involve increased risk of computers, mobile devices and other devices getting infected with malicious software;
- regular updating of antivirus programs;
- accessing the Service exclusively via the web address specified in the User instructions;
- checking regularly for new notifications sent by the Bank through the Service or in another agreed or prescribed manner, and comply with and act in conformity with such notifications;
- [the User shall be obliged] to promptly notify the Bank of a change of the mobile phone number of an End User in order to ensure secure functioning of the Service (sending of an SMS message for the purpose of SMS authorisation, as well as sending of an SMS message which contains an Identification Code needed for activation of the PBZ mobile banking application).

2. The User shall cover any potential damage caused by non-compliance with these provisions by the User and/or [any damage that may arise] if a third party has in any way come into possession of devices and/or data related to authorisation by the User/End Users in the system of PBZ digital banking (e.g. Payment Instruments, user names, passwords, codes, PINs, and other identifiers).

3. The User shall bear the entire risk of incorrect data entry in all documents referred to in these General terms for digital banking.

4. The User shall bear the risk and shall be liable for instructions provided in the payment order which the User has authorised in conformity with these General terms and the User instruction.

10. BLOCKING OF A PAYMENT INSTRUMENT

1. In the event of loss, theft, misuse or unauthorised use of a Payment Instrument or of suspected unauthorised use of the Service, the User/End User shall without delay notify the Bank of any such loss, theft, misuse or unauthorised use of a Payment Instrument or of suspected unauthorised use of the Service.



2. The User shall be liable for and shall bear the damage caused by unauthorised payment transactions, regardless of the amount of a transaction, executed by using Payment Instruments, which (unauthorised transactions) are the consequence of loss or theft or unauthorised use or misuse of a Payment Instrument, up until the moment when the loss or theft or unauthorised use or misuse of a Payment Instrument is reported to the Bank.

The reporting of the loss or theft or unauthorised use or misuse of a Payment Instrument shall be done in writing, by contacting the organisational unit responsible for managing the business relationship with the User or via the Bank's Call Centre (valid phone numbers of the Bank's Call Centre are posted on the website of the Bank).

If a security device or the application software is installed on a mobile device, it is necessary to report the loss of the mobile device to the Bank in the manner described above.

3. The Bank shall be authorised to block a Payment Instrument and/or the Service referred to in the previous paragraph for objectively justifiable reasons:

- 1) related to security of a Payment Instrument (for example, skimming),
- 2) related to suspected unauthorised use, or use of a Payment Instrument and/or the Service with the intention to commit fraud and/or to misuse a Payment Instrument and/or the Service,
- 3) in the case in which the Bank provides the Payment Instrument service including a credit line, for reasons related to a significantly higher risk that the payer/User will not be able to meet its payment obligation.

4. The Bank shall, if possible, inform the User of the intention to block a Payment Instrument and of reasons for blocking of a Payment Instrument ahead of the very blocking, by phone and/or in writing or in another suitable way.

If the Bank is unable to inform the User of the intention to block a Payment Instrument and of reasons for blocking before it occurs, the Bank shall do it after blocking of a Payment Instrument, by phone and/or in writing or in another suitable way. The Bank shall not be under an obligation to inform the User about the blocking of a Payment Instrument if this runs counter to objectively justifiable security reasons or is in contravention of law.

5. The Bank, as the payment system provider holding the account, shall be authorised to deny access thereto to an account information service provider or a payment initiation service provider on the basis of proven and objectively justifiable reasons that are related to unauthorised access with the aim of committing fraud, including unauthorised payment transaction initiation or payment transaction initiation aimed at committing fraud. The Bank shall notify the User that access to the transaction account is denied to the account information service provider or the payment initiation service provider by phone and/or in writing or in other appropriate manner, except in cases where such notification would be contrary to objectively justifiable security reasons or regulations.

6. Payment orders issued and sent to the Bank before the blocking of a Payment Instrument and/or the Service shall be executed.

7. For reasons stated in paragraph 3, items 2 and 3 of this Article, the Bank shall be authorised also to cancel the Contract in writing, without any notice period. In that case, the User shall be required to pay to the Bank all fees and costs incurred during the use of a Payment Instrument and to return the said Payment Instrument together with all the equipment handed over to the User by the Bank for the purpose of enabling the use of the Payment Instrument.

8. For reasons stated in paragraph 3, items 2 and 3 of this Article, the Bank shall be authorised to cancel in writing, without any notice period, also the Framework Contract. In that case, the User shall be required to pay to the Bank all fees and costs incurred during the use of a Payment Instrument and to return the said Payment Instrument together with all the equipment handed over to the User by the Bank for the purpose of enabling the use of the Payment Instrument.

9. The Bank shall not be liable for any damage that may be done to the User due to blocking of a Payment Instrument and/or the Service, where such blocking has been undertaken for reasons stated in this article.

11. FEES

1. For the duration of the Contract, the Bank shall calculate and collect a fee for contracting and use of the Service in accordance with the Decision on fees in transactions with domestic and foreign business entities, individuals and financial institutions (hereinafter: the Decision on fees), as defined in the General operating terms for transaction accounts.

2. For the execution of payment transactions through the Service, a fee per transaction shall be calculated and collected in accordance with the General operating terms for transaction accounts and the Decision on fees, as defined in the General operating terms for transaction accounts. For the performance of other services through this Service, a fee shall be calculated and collected in accordance with the General operating terms for transaction accounts and the Decision on fees, as defined in the General operating terms for transaction accounts.

3. The User, by signing the Contract, authorises the Bank to debit the amount of the calculated fee due and payable and/or other costs against the User's transaction account(s) held at the Bank on the value date i.e. the due date of payment, without any further User's consent being required. If there are no sufficient funds in the local currency in the User's transaction accounts, but there are sufficient funds in a foreign currency, the Bank shall be authorised to collect the payment out of foreign currency funds, carrying out a currency conversion in which the mean exchange rate from the Bank's exchange rate list effective as of the date of fee collection shall be applied as the agreed exchange rate.

4. The User shall be obliged to provide sufficient funds in the User's transaction accounts that were designated by the User as the accounts for fee collection in the *Request for the use of PBZ digital banking for business entities* in order to enable collection of the fee for the use of the Service in accordance with the General operating terms for transaction accounts. The amount and type of fees, as well as other costs that may be incurred as a result of the performance of the Contract for



the use of PBZ digital banking for business entities, shall be subject to change in accordance with the provisions of the General operating terms for transaction accounts.

12. TERMINATION OF THE SERVICE USE

1. The Contract for the use of PBZ digital banking for business entities shall be concluded and shall remain in force for an indefinite period.

2. The contractual relationship shall be terminated in conformity with the provisions of the Contract. Also, the Contract shall be terminated if the User ceases to exist and/or if the User who is an individual i.e. a natural person ceases to transact business or to render professional services as a self-employed professional, and/or upon death of the said natural person who transacted business as a sole trader or a self-employed professional, and/or if the User is dissolved by a decision of the court or decision of another competent body or by law or on the basis of other regulations.

13. FINAL PROVISIONS

1. These General terms for digital banking are available through the business network of the Bank, and on the website of the Bank (www.pbz.hr).

2. The Bank and the User agree that they shall, in conformity with the Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS Regulation) mutually acknowledge in a court of law the validity of electronic messages that are to be generated within the scope of particular electronic banking services.

3. The Bank reserves the right to amend these General terms for digital banking. The Bank shall provide the User with the amendments to the General terms for digital banking, including the change of the title of General terms for digital banking or replacement with the new terms, in writing or via telecommunication/electronic channels at least 15 days prior to entry into force of the amendments to the General terms for digital banking, the new general terms or other internal documents of the Bank to whose application these General terms for digital banking refer. It shall be deemed that the User has accepted the amended terms if, by the proposed date of their entry into force, the User has not informed the Bank in writing that it/he/she does not accept them.

4. If the User notifies the Bank in writing, within the period of time referred to in the previous paragraph of this article, that it/he/she does not accept the amendments to the General terms for digital banking and/or internal documents of the Bank to which the General terms for digital banking refer, it shall be deemed that the User does not wish to continue business cooperation with the Bank, and the User shall, before the proposed date of amendments to the General terms for digital banking, be required to cancel the Contract, to pay all due and payable amounts to the Bank and to return Payment Instruments together with the equipment, if under the said Contract they have been placed at the User's disposal.

5. By signing the Contract and the Request for the use of the Service, pursuant to the provisions of the Credit Institutions Act, the User, as legal entity, gives consent to the Bank to forward all data on the User as the legal entity, to which the Bank gains access during performance of transactions provided for in the Contract to the central database of its group in the Republic of Croatia and abroad, and they agree that all the group members may have access to and use these data.

6. The Bank, as a data controller, operates in accordance with the principles of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). When personal data of the Bank's clients are collected, whether from a client at the time of collection or from another source, the Bank shall provide information in accordance with Articles 13 and 14 of the General Data Protection Regulation, such as, for example, information about the Bank as the controller, the purposes and the legal basis of personal data processing, the categories of personal data which are collected (for example, personal data required for the establishment of a business relationship pursuant to the Anti-Money Laundering and Terrorist Financing Act, as well as other data necessary for the performance of a particular contract or for taking actions prior to entering into a contract or for the fulfilment of some other legal obligations, legitimate interests of the Bank as the controller or of a third party); [information about] the storage period, the recipients of data, the source of data, as well as the rights related to personal data protection (for example, the right of access to personal data, the right to erasure, the right to object, etc.), where such information shall be provided through the document "Information on the processing of personal data of natural persons in transactions with legal entities", available to clients at www.pbz.hr and at the premises of the Bank. Contact details of the data protection officer: sluzbenik.za.zastitu.osobnih.podataka@pbz.hr.

If processing is based on consent as the legal basis for processing, then the User, an End User, an authorised representative or other natural person involved in the conclusion and/or performance of the Contract may at any time withdraw his or her consent. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

The Bank shall collect and process personal data for the purpose of the implementation of the Law on administrative cooperation in the field of taxes, which governs the implementation of the Agreement between the Government of the Republic of Croatia and the Government of the United States of America to Improve International Tax Compliance and to Implement FATCA (the Foreign Account Tax Compliance Act, the US law which introduced a reporting obligation for



financial institutions with respect to certain accounts), which includes collecting of information, application of the due diligence rules, identification of US reportable accounts, as well as reporting on these accounts to the Ministry of Finance. The Bank shall collect and process personal data also for the purpose of the implementation of the Law on administrative cooperation in the field of taxes, which governs administrative cooperation in the field of taxes between the Republic of Croatia and EU Member States as well as automatic exchange of information on financial accounts between the Republic of Croatia and other jurisdictions, within the framework of the so called Common Reporting Standard (CRS), which includes collecting of information referred to in Article 26 of the Law in accordance with the reporting rules and the due diligence rules, identification of reportable accounts, as well as reporting on these accounts to the Ministry of Finance, Tax Administration.

7. These General terms for digital banking have been drawn up in Croatian and in English. In the event of any discrepancy between the texts in Croatian and in English, the Croatian version shall prevail.

8. The language of communication between the User/End Users and the Bank for the duration of the Contract shall be the one specified in the Contract.

9. At the date of entry into force of these General terms for digital banking, the Service may be contracted at the Sinergo desk by business entities with a transaction account with the Bank, while contracting the Service via PBZCOM@NET electronic banking services shall be available to a certain category of business entities upon meeting the criteria in accordance with the business decision of the Bank and the technical conditions for contracting and using the Service.

10. These General terms for digital banking shall enter into force on May 25, 2025, and are adopted for the purpose of defining the method of displaying the PIN for a debit card for business entities in the mobile banking application of the Service, as well as the method of activating an inactive debit card for business entities via the PBZ mobile banking application and the PBZ internet banking application.

The General terms for digital banking from May 16, 2023 are repealed with the date these General terms take effect.

In Zagreb, April 17, 2025