

UniCredit Bank Hungary Zrt.'s General Terms and Conditions

Effective from
10th December 2020

TABLE OF CONTENTS

4	I. GENERAL PROVISIONS
4	1. Introductory provisions
5	2. Definitions
8	3. Representation
11	4. Orders
14	5. Date and place of performance
14	6. Bank secret, management of personal data, data supply to third parties
20	7. The Bank's liability
21	8. Use of agents
21	9. Cooperation, information, notification
23	10. Verification of and objections to the Bank's notifications
24	11. Complaint management
26	12. Interests, fees, commissions and costs
27	13. Jurisdiction and applicable law
28	II. TELEPHONE AND ELECTRONIC BANKING SERVICES
28	1. Common provisions
28	1.1. Definitions
29	1.2. Use of the Services
30	1.3. Liability
33	1.4. Termination of the Service Agreement
34	1.5. Fees, charges and costs
35	2. Telephone Banking Services
40	3. Electronic Banking services I. (Internet Banking and SpectraNet Mobil Banking)

General Terms and Conditions

50	4. Electronic Banking Services II. (Home Banking)
54	5. Electronic Banking services III. (UniCredit mBanking mobileapplication and Private Invest Application)
54	5.1. Definitions added to Section I. 2 (Definition) of the Terms and Conditions
55	5.2. Activation of services
57	5.3. The use of the system and its services
60	5.4. Security
61	5.5. Deactivation
62	III. SPECIAL PROVISIONS REGARDING CERTAIN FINANCIAL AND ADDITIONAL FINANCIAL SERVICES
62	1. Payment account maintenance
85	2. Opening of deposits
88	3. Collection of postal fee for postal cash services
88	4. Cheque
89	5. Foreign currency trading
89	6. Custody service
89	7. Safe service
89	8. Credit reference service
89	9. Brokerage of financial services
90	10. Currency exchange
90	11. EFER Service
91	IV. EFFECT OF THE GENERAL TERMS AND CONDITIONS
92	ANNEX 1. OUTSOURCED ACTIVITIES
94	ANNEX 2. DATA CONTROLLING GUIDELINES

UniCredit Bank Hungary Zrt.'s General Terms and Conditions

Effective from 10th December 2020

I. GENERAL PROVISIONS

1. Introductory provisions

- 1.1. These General Terms and Conditions (hereinafter: General Terms and Conditions) include general terms and conditions for legal transactions between UniCredit Bank Hungary Zrt. (seat: 1054 Budapest, Szabadság tér 5-6., number of operating licence: I-1400/2001. issue date of operating licence: 10 August 2001. and I-1523/2003. on 1st December 2003. No. of original operating licence: F-20/1992. dated 28 February 1992.) (hereinafter: Bank) and its Clients with a binding effect upon both the Bank and the Client without any specific stipulation, unless any individual agreement or the special regulations applying to different transaction types of credit institutions (Terms and Conditions for Retail/Corporate Clients, Bank Card Terms and Conditions, General Terms and Conditions for Investment Services and Additional Services) (the Terms and Conditions and the above regulations shall be hereinafter jointly referred to as: Business Regulations) provide otherwise. The general provisions of these Terms and Conditions shall apply in cases where the special business regulations relating to the transaction types of credit institutions or – in the absence of such regulations – the special provisions of these Terms and Conditions pertaining to the given activity do not provide otherwise.
- 1.2. The authority supervising the Bank is the National Bank of Hungary (1013 Budapest, Krisztina krt. 39.)
- 1.3. In matters not regulated by the specific agreement between the Bank and the Client, business regulations relating to the particular transaction types of credit institutions shall apply. In the absence of such regulations, these Terms and Conditions, or in matters not regulated therein, the provisions of prevailing legislation shall be applicable. With regard to certain banking transactions – especially for orders related to foreign trade – the appropriately published/announced international agreements and regulations (standards) shall also apply.
- 1.4. The Business Regulations are public information, and may be viewed by anyone on the Bank's web site: www.unicreditbank.hu or at the premises of the Bank open to Clients. The Bank shall make its Business Regulations available to the Client upon request, free of charge.
- 1.5. The List of Conditions is an inseparable part of these Terms and Conditions.
- 1.6. In the case of clients qualifying as consumer or micro-enterprise, the Bank may initiate the modification of the Framework Agreement concerning cash services at least two months before the modification takes effect. Detailed rules regarding the modification of the Framework Agreement are contained in section "Amendment of the Framework Agreement" of these Terms and Conditions.
- 1.7. For agreements concluded between the Bank and the Client for the purpose of loan or any other financial services, the Bank's rights to the unilateral modification of contracts are governed by the provisions of the Bank's Terms and Conditions for Retail Clients as well as of the Bank's Terms and Conditions for Corporate Clients and Municipalities.
- 1.8. The Bank reserves the right to unilaterally amend the Terms and Conditions and the List of Conditions whenever a new service is launched. Such supplements and amendments shall also apply, from the moment they come into force, to contracts already concluded.
- 1.9. Should any provision or part of a provision of any contract concluded between the Bank and the Client become invalid or unenforceable, this shall not affect the validity of the remainder of the contract. In such cases, the Bank and the Client shall replace the invalid or unenforceable provision with a valid or enforceable provision that is as close as possible in terms of business content and purpose to the provision being replaced.

2. Definitions

1. **“Data Protection Act”** shall mean Act CXII of 2011 on Informational Self-Determination and Freedom of Information.
- 1/A **“General Data Protection Regulation”** means 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.”
- 1/B **“processing”** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- 1/C **“controller”** means the natural or legal person, public authority, agency or other body, including particularly the Bank, which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
- 1/D **“Alternative Benchmark”** means any benchmark rate (inclusive of any spreads or adjustments) which is formally designated, nominated or recommended as a replacement by a Relevant Nominating Body.
2. **“Transfer”** shall mean a payment service conducted upon instruction of the Client as paying party, where the account of the Client as paying party is debited in favour of the beneficiary; it may also refer to official transfers as well as to transfers based on summons.
3. **“Signature Card”** shall mean a document signed and submitted by the Client to the Bank which is designed by the Bank and forms an inseparable part of the Framework Agreement, containing the model signatures of authorized signatories in connection with the agreement, issued upon conclusion of the agreement or thereafter between the Client and the Bank.
4. **“Agreements subject to data supply”** in accordance with Section 2, Art. 5 of the CCIS Act shall mean credit/ financial loan agreements, the issuance of non-cash payment instruments and the provisions of related services, undertaking of guarantees or bank guarantees or any other banker’s obligations, the provision of investment loans or securities lending as well as student loan agreements as defined by law.
5. **“Bank Business Day”** shall mean a day on which the Bank conducts business activities as per its effective opening hours, so when the Bank is open for the purpose of executing payment transactions.

The Bank shall operate 24 hours a day, every calendar day without any interruption in order to carry out its duties regarding instant payment transfers defined in Decree 35/2017 (XII. 14.) MNB on Payment Services Activities – including the debit or credit value date for the amount of the payment transactions, the due date for interest payments on overdraft facilities and the date on which the overdraft interest is credited, and the charge of fees due on the last Bank Business Day of the calendar month according to the effective List of Conditions– unless an act or decree provides otherwise.
6. **“Bank Holiday”** shall mean a day, which does not qualify as a Bank Business Day, on which the Bank does not carry on business.
7. **“Domestic Payments Activity”** shall mean all payment transactions in which the payment service provider of both the paying party and the beneficiary provide their payment services within the boundaries of Hungary.
8. **“Collection”** shall mean a payment service provided upon the beneficiary’s instructions where debiting of the paying party’s Payment account in favour of the beneficiary shall take place on the basis of the paying party’s consent given to the beneficiary, to the beneficiary’s bank or to the paying party’s own bank.
9. **“Bsz.”** shall mean the Act CXXXVIII of 2007 on investment enterprises and commodity market service providers as well as on the rules of activities they may perform.
10. **“Breakdown of Costs”** shall mean a document making part of the Account Statement which contains an itemized list of all fees, costs and other payment obligations related to the payment services, payable by the Client being a client qualifying as consumer or micro-enterprise to the Bank.
11. **“Personal Identifier”** shall mean the payment account, or in the absence thereof any combination of letters,

numbers or symbols assigned to the Client by the Bank for the purpose of clear identification of the beneficiary.

11/A. "Strong Customer Authentication" shall mean an authentication based on the use of two or more elements categorised as

- a) knowledge, which is something only the Client knows,
 - b) possession, which is something only the Client possesses, and
 - c) inherence, which the Client is
- that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data.

12. "EEA State" shall mean any Member State of the European Union or any other state that is party to the Agreement on the European Economic Area.

13. "EEA Currency" shall mean the official currency of an EEA State.

14. "Payment Transaction within EEA" shall mean a payment transaction where the payment service provider of both the paying party and the beneficiary, or the sole payment service provider performing the transaction provide their services in the territory of the EEA.

15. "Value Date" shall mean the day which is taken into account by the Bank for the calculation of interests for any amount debited or credited to the Payment account.

15/A. "Payment Initiation Service" shall mean a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider.

15/B. "Payment Request" Upon agreement between the Beneficiary Account Holder and the Bank, the Beneficiary Account Holder may initiate an instant payment transfer from the Payer in the form of a payment request submitted to the Bank. If the Bank maintains the payment account of the Payer Account Holder, it shall promptly forward the payment request received to the Payer Account Holder, in accordance with the agreement and arrangement with the Payer Account Holder. At present, the Bank does not provide any services related to payment request for its Clients.

16. "Paying Party" shall mean any entity

- a) which, as the owner of the payment account, approves any payment order to be executed from its payment account, or

- b) which submits a payment order in the absence of any payment account, or
- c) whose payment account is debited due to any official transfer order or to any transfer based on summons.

17. "Payment Order" shall mean any instruction by a payer or payee to his payment service provider requesting the execution of a payment transaction, including official transfer orders and remittance summons.

18. "Payment Transaction" shall mean the execution of any order initiated by the paying party, the beneficiary, the person authorized to issue official transfer orders or the issuer of the summons for transfer, following a certain method of payment, irrespective of the legal relationship between the paying party and the beneficiary.

19. "Payment Account" shall mean any account opened in the name of the Bank's Client for the purpose of executing payment transactions specified by relevant legislation or these Terms and Conditions; this may include bank accounts, current accounts, cash accounts and accounts for limited purposes as well.

20. "Business Organization" shall mean any legal entity excluded the consumers.

21. "Authentication" shall mean a process enabling the Bank to verify the identity of the Client or the validity of the use of a specific payment instrument, including the use of the Client's personalised security credentials.

22. "Hpt." shall mean the Act CCXXXVII of 2013 on credit institutions and financial undertakings.

22/A. Third Party Provider (TPP) Third Party Providers are market participants (offering payment initiation and/or account information services) who are entitled to use the open API in order to obtain banking data and/or initiate payment transactions for customers with an online accessible payment account – after obtaining the appropriate licenses and customer authorizations (consent).

23. "Written Form" shall mean any written amendment to the framework agreement, including any modification of limits through recorded phone conversations, with the stipulation that limit modifications made over the phone shall be subsequently confirmed in writing by parties at any time upon request of either party.

- 24. “Language of Communication”** shall mean the language of the banking service agreement making part of the Framework Agreement.
- 25. “Beneficiary”** is the entity that is entitled to funds concerned by the payment transaction.
- 26. “Framework Agreement”** shall mean an agreement incorporating all business regulations, lists of conditions, announcements, forms designed by the bank, the List of Conditions and the table of exchange rates pertaining to the payment service provided (including the agreements related to the Service), concluded between the Bank and the Client, which determines all essential conditions for payment orders and payment transactions (including the opening of payment accounts) based on the framework agreement, for a given period and, only for the purposes of the Private Invest Application, an agreement concluded for the provision of investment services.
- 27. “CCIS”** shall mean the central credit information system recognized by the National Bank of Hungary (in Hungarian: “KHR”).
- 28. “CCIS Act”** shall mean Act CXXII of 2011 on the Central Credit Information System.
- 29. “List of Conditions”** shall mean the set of conditions set forth in lists of conditions and announcements published in the manner required by the relevant legislation and these Terms and Conditions, pertaining to non-individual transactions between the Bank and the Client.
- 29/A. “Relevant Nominating Body”** means the applicable central bank, regulator or other supervisory authority having the competence towards the Bank and/or the administrator and the publisher of the Benchmark, or any institution designated by them.
- 29/B. “Batch order”** shall mean, in terms of instant payment transfers, all transfer orders where the Bank receives more than one payment order from the Customer at the same time or the Customer consents more than one payment order at the same time.
- 29/C. “Central Database”** means the register of the Account Holder’s Name, IBAN, and Secondary Account Identifier as disclosed by the person having the right to dispose over the account.
- 29/D. “Secondary Account Identifier”** means the unique identifier disclosed by the person having the right to dispose over the account through the Bank to the organization operating the Central Database that allows the clear identification of the Customer’s payment account.
- 30. “Micro-enterprise”** shall mean any legal entities and unincorporated business organizations which – at the time the framework agreement is concluded, based on the information at the Bank’s disposal – have a total headcount of less than 10, and whose annual turnover or balance sheet total in the business year preceding the year when the agreement is concluded is not more than EUR 2 million or HUF equivalent based on the official exchange rates posted by the National Bank of Hungary on the last day of the business year preceding the year when the agreement is concluded.
- 31. “International Customs”** shall mean among others the “Uniform Customs and Practice for Documentary Credits”, the “Uniform Rules for Collections”, the “Uniform Rules for Contract Guarantees” and the “Uniform Rules for Demand Guarantees”, as amended time to time, issued by the International Chamber of Commerce, 38 Cours Albert 1er, 75008 Paris (hereinafter jointly referred to as: “ICC rules”).
- 31/A. “Payment Account Accessible Online”** shall mean a payment account, regarding of which it is possible to give Payment Orders or access data and information by direct connection of information technology device.
- 32. “Complaint”** shall mean the objection of the Client to any action or omission of the Bank relating to the pre-contractual phase, or the conclusion of the agreement, the fulfilment of the agreement by the Bank, and the termination of the contractual relationship respectively hereinafter the settlement of the legal dispute with respect to the agreement.
- 33. “Cash Account”** shall refer to the Payment account opened or having been opened by the Account Owner for the purpose of conducting transactions within the framework of its regular business activities, based on an obligation stipulated by law.
- 34. “Pft.”** shall mean the Act LXXXV of 2009 on providing payment services.
- 35. “Pmt.”** shall mean the Act LIII of 2017 on the prevention of money laundering and terrorist financing.
- 36. “Reference Data”** shall mean any information, including the personal particulars of a registered person, which may be handled by the financial enterprise managing the Central Credit Information System in accordance with the Hpt.

37. “Reference Data Provider” shall mean the institution recognized by the CCIS Act as reference data provider.

37.A. “Reference rate” means the reference rate used to determine the contractual interest rate or the reference amount used to determine the amount to be paid under any transaction.

38. “Making available” shall mean a method of providing information to clients by the Bank where the Bank makes subsequent information available to the Client upon the Client’s request once in a month free of charge through Internet Banking or SpectraNet Mobil Banking, or send it by post upon the Client’s request submitted through Telebank, or by delivering it in person to the Client upon his/her request in a branch.

38/A. “Account Information Service” shall mean an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service providers.

39. “Account Statement” shall mean subsequent information sent to the Client in relation to any Order executed in the Client’s Payment account based on the Framework Agreement, or any Order executed without using any Payment account if the Client has no Payment account maintained with the Bank.

39/A. “Fee Statement” means the document prepared and handed over annually by the Bank to Clients qualifying as consumers in accordance with provisions of Government Decree 144/2018 (VIII.13.) on certain issues related to the disclosure of fees related to payment accounts held for consumers, which shall contain all fees, costs and, where applicable, the interest rates applied to the Payment Account related to the use of the.

40. “Account Holder” shall mean a natural person, or Business Organization to which the Bank provides payment services, has a valid Payment account agreement or consolidated securities account agreement with the Bank, or is a card holder having a credit card agreement.

40/A. “Personalised security credentials” shall mean personalised features provided by the Bank to the Client for the purposes of authentication.

40/B. “personal data” means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference

to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

41. “Durable Medium” shall mean any instrument which enables the Client to store information addressed personally to him/her for a period of time adequate for the purposes of the information and which allows the unchanged reproduction of the information stored.

41/A. “Remote Payment Transaction” shall mean a payment transaction initiated via internet or through a device that can be used for distance communication.

42. “Distance Communication” shall mean any method making it possible to make a statement of agreement in the absence of parties for the purpose of concluding a framework agreement or a one-off agreement for a payment transaction.

43. “Order of Performance” shall mean the document forming an inseparable part of the List of Conditions, in which the Bank sets out the dates (Value Dates) by which it completes the tasks arising from the performance of Orders.

44. “Client” shall mean any private individual, legal entity, unincorporated business organization or any other organization for whom/which the Bank provides financial, supplementary financial, investment or supplementary services; this definition also includes the Account Owner.

3. Representation

3.1. Pursuant to Pmt, the Bank is obliged to identify the Client – together with authorized representatives – by means of vetting, and in doing so the Bank is entitled to verify the personal identity of the Client, its proxy holder, the persons with rights of disposition, and any representative. For this purpose, the Bank shall require the documents listed in the below section I.3 to be presented and also verify their validity. Pursuant to Pmt, the Bank shall make a photocopy of such documents and certificates.

3.2. The Bank shall apply client vetting as per section I.3.1 in the events defined in Pmt (among others, when entering into a business relationship, or if a transaction order reaches a limit specified in any legislative provision).

- 3.3. When establishing the identity of a person, the Bank shall require the following documents to be presented by the Client:
- a) in the case of a natural person:
 - aa) an official document held by a Hungarian citizen suitable for certifying his/her identity (that is, identity card, passport, or driving licence in a card format) and an official document certifying the home address,
 - ab) in the case of a foreign natural person, a passport and a personal identification card provided that it entitles him/her to stay in Hungary, or any other document certifying or granting a right of residence,
 - b) in the case of a legal entity or unincorporated organization, the person authorized to proceed in the name or upon instruction of the organization shall present – in addition to the document specified in sub-section a) of this section – a document not older than 30 days, proving that:
 - ba) in the case of a domestic business organization, that it has been registered by the Court of Registration, or submitted an application for registration; or, in the case of a sole trader, that a sole trader's licence was issued or the certificate of the registration was issued,
 - bb) in the case of a domestic legal entity, that it has been recorded by the authorities or the court if this is required for the entity to be established,
 - bc) in the case of a foreign legal entity or unincorporated organization, that it has been registered or entered into the official records in accordance with the law of the country in which it is based;
 - c) the deed of foundation of the legal entity or unincorporated organization (articles of association, bylaws) prior to its submission to the court of registration, the authorities, or the courts, of its application for registration by the court of registration, the authorities, or the courts. In this case, the legal entity or unincorporated organization shall submit a document to the Bank, certifying that it was duly incorporated or entered into official records within 30 days following incorporation or registration by the authorities or the courts; furthermore, the Bank shall record the company registration number or any other registration number of the organization. In doubtful cases, the Bank is entitled to request additional documents.
- 3.4. The authorization for representation must be certified by a public document or a private document providing full evidence. It shall be indicated in the letter of ad hoc authorization, which specific matter(s) the authorization extends to.
- 3.5. Personal identity and/or the right of representation may – based on a statutory provision, an international agreement, the Business Regulations or the provisions of the agreement between the Bank and the Client – also be certified by means of other documents.
- 3.6. If the Client submits a foreign language document to the Bank to prove his/her identity or right of representation or any other fact, the Bank shall be entitled to request an authenticated Hungarian translation of such document or to have it translated at the Client's expense. The Bank shall not be liable for any damage arising from the inspection or translation of such document.
- 3.7. When performing a client vetting, the Bank shall record the following data:
- a) natural persons
 1. first name and family name (name at birth) and the married name, if any,
 2. home address, in the absence of home address, place of residence,
 3. date and place of birth,
 4. nationality,
 5. mother's maiden name,
 6. type and number of the identification document,
 - b) legal entity or unincorporated organization
 1. name and abbreviated name,
 2. the registered seat, or the address of the branch office in Hungary if the company is registered abroad,
 3. in the case of a legal entity registered with the Court of Registration, the company registration number, or in the case of other legal entities the number of the decision on its establishment (entering into records, incorporation) or its registration number,
 4. core activity,
 5. names and positions of persons with rights of representation,
 6. the identification data of the service agent;
 7. tax number;
 - c) the most important data of and related to the business relationship and the transaction order.
- 3.8. The Client shall make a written declaration to the Bank to the effect that it acts on his own or on behalf and interest of its actual owner (within the meaning of the Pmt). The person acting on behalf a legal entity or an unincorporated organization is obliged to make a written statement of the actual owner. Should any doubt arise at any time regarding the identity of the actual owner, the Bank shall call upon the Client (repeatedly) to give a written statement on the actual owner.
- 3.9. Prior to entering into a business relationship or executing a transaction order, or – if it is necessary to avoid any interruption in the normal course of

business, and money laundering or terrorist financing is unlikely to occur – at latest by the date of execution of the first transaction order, the Bank shall carry out the verification of identity of the Client and the actual owner. If the Client is a legal entity or an unincorporated organization, following vetting of the person acting on its behalf or upon its instructions, it is also necessary to carry out the vetting of the legal entity or unincorporated organization itself.

The Client who is obliged to make a written statement to the Bank, specifying whether he/she is considered a politically exposed person. If she/he is qualified as a politically exposed person, the statement shall contain, under which provision of the Pmt he/she is considered as such and the information on the sources of the funds. The same information shall be provided regarding the beneficial owner(s).

- 3.10. The Client shall inform the Bank in writing or in person of all changes in the data recorded during client vetting or in the person of the actual owner according to Pmt within five working days after he/she obtains knowledge of such changes. The Bank shall accept no liability in the event that the Client does not provide notification of changes in such data, or does so too late, or provides incorrect data, or if the Client has originally supplied incorrect or false data. If no client order was executed on the account of the Client kept at the Bank for two calendar years – with the exception of transactions with multiyear duration –, the Bank shall call the attention of the Client within 30 days in writing to disclose to the Bank any change in his/her data, together with the notification that the Bank shall not execute any Client order until the disclosure of the data.
- 3.11. The Bank shall record and keep all data and documents that come to its knowledge concerning the Client upon performance of client vetting during the life of their contract relationship as well as for a period of eight years following termination thereof.
- 3.12. The Client acknowledges that if the Bank is unable to perform client vetting as specified in section I.3 of these General Terms and Conditions – including the case where the Client does not agree to the identification procedure making part of vetting or to the verification of his/her identity, or if client vetting under Pmt. cannot be performed due to any other reason, or if the client refuses to make a statement concerning his/her status as a politically exposed person –, the Bank shall refuse to execute the transaction ordered by the Client through the Payment account for the given Client, or shall refuse to enter into a business relationship or to perform any transaction order, or shall terminate the business relationship existing with that Client.
- 3.13. The Bank shall regard the representatives registered with it as the Client's representatives until any competent department of the Bank receives written notification of withdrawal of the right of representation in a form accepted by the Bank, supported by appropriate documents. The Bank shall not be liable with respect to any damages that occur in the course of the performance, non-performance or late performance of the Client's instructions due to any legal disputes arising on the Client's side in relation to the changes in the right of representation of the Client.
- 3.14. Any restriction of the power of representation vested upon the Client's authorized representative shown in the relevant registry, or rendering such representative's actions conditional or subject to approval shall only be effective as against the Bank, if the Client expressly notifies the Bank of the restriction, or the necessity of approval or a condition to occur.
- 3.15. The Client shall provide the Bank with a duly issued Signature Card, and undertakes to inform the Bank of any changes in the content of the Signature Card without delay. The Bank shall keep an electronic record of the signatures of the Client, its representative, the person with rights of disposition and any other person specified by the Client as a permanent proxy holder. The Bank is obliged to check the authenticity of signatures on all of the Client's written instructions. The Bank shall compare the signature on each written instruction with the specimen signature recorded electronically. If the instruction is not signed in the manner recorded with the Bank, the Bank shall be entitled to return the instruction to the Client together with an explanation, and shall not be liable for any damages arising therefrom.
- 3.16. The Bank is entitled to ask its Clients for a proxy in the form of a public document or a private document providing full evidence. Should the conditions of the proxy – according to the Bank's judgment – not be sufficiently clear, or should there be a need to examine other documents in addition to the instrument of proxy or the conditions indicated in the instrument of proxy in order to interpret its content, or should the Client provide the proxy in a manner that is not customary at the Bank, or otherwise disregard the format and content requirements, the Bank shall not be obliged to perform the instruction given based on the proxy. General proxy for cash withdrawal shall be signed solely by the Client

(statutory representative) with rights of disposition on the account. Occasional proxy for cash withdrawal shall be signed solely by the person with rights of disposition who signed the concerned cash withdrawal order.

- 3.17. The specimen signatures of employees acting on behalf of the Bank in a given case shall, upon the Client's request, be made available to the Client for inspection in the Bank's premises.
- 3.18. The Bank states that the head of department lacking the legal status of a legal person is not vested with individual power of representation in matters considered necessary for the regular functioning of the department.
- 3.19. In case of the Client's involuntary de-registration procedures, the Client acknowledges that any person who is entitled to dispose over the bank accounts and securities accounts held by the Bank may only exercise such right of disposal if the Client makes an advance written declaration to the Bank stating that such persons, when disposing over such accounts, will act in accordance with the provisions and limitations applicable to the involuntary de-registration procedures and the Client takes the liability for that. The Bank excludes its liability for any damages arising from the violence of the applicable laws.

4. Orders

- 4.1. The order shall clearly specify the exact name of the Client, the subject of the transaction and all data necessary for the transaction to be executed, prescribed by the Bank, the international rules applying to payment transactions (e.g. SEPA Rulebook), legislative provisions and International Customs. If the Client has provided incorrect or insufficient data for executing the order, or if the order is incorrect from the linguistic point of view, the Bank shall not be liable for any damage that arises as a result. On the other hand, in the case of incoming payment orders to perform against the Client's bank account, the Bank shall verify whether the name and number of the Payment account to be debited match those of the account owner's account according to the registry of the Bank except in the case of submitting instant transfer orders, where the Bank may not refuse the receipt of the instant transfer order on the grounds that the payer has provided a secondary account identifier instead of the payee's name and account identification number.
- 4.2. The Bank shall not be liable for any damage arising from the fact that the various copies of the payment order have been filled out differently by the principal,

or that the person submitting the order has misled the Bank or the Client. In terms of performance, the copy of the payment order that remains with the Bank shall be regarded as the authentic one.

- 4.3. The Bank shall, if requested, forward the documents related to the performance of orders concerning documentary and guarantee transactions (including bill of exchange, other securities, etc.) – pursuant to international rules by a method selected with due care as it may reasonably be expected of it – at the Client's risk and expense.
- 4.4. The Client is entitled to submit his/her orders to the Bank in writing (by post, or by submitting a form in the Bank's branches), or based on a separate agreement via the Bank's electronic banking or telephone banking services or via a payment initiation service provider. The Customer shall be entitled to submit an immediate transfer order to the Bank only electronically. For orders that are not submitted on the form applied by the Bank, the Bank shall be entitled to charge a separate fee as specified in the List of Conditions. The Bank shall be entitled to return any orders submitted with a signature error, illegible content or missing data without the order being executed.
- 4.5. Electronic letters that have been sent via any computer network to the Bank's electronic mailing address shall not be considered as orders.
- 4.6. In the interest of the secure fulfilment of orders given over the telephone, the Bank may in certain cases request that the Client confirms the order, prior to fulfilment, by telephone or by fax. The Bank shall not be liable for any damages resulting from any mistake, misunderstanding or error that occurs due to any reasons emerging on behalf of the Client during the transfer of information using the telephone or by fax – including the eavesdropping of the phone calls by unauthorized persons.
- 4.7. The Bank is entitled to transform the type of the payment order into another – except for instant transfer orders –, executable payment order type. The transformation is solely allowed in order to facilitate the performance of the payment order or the optimization of the choice of the settlement systems available for the performance of the payment order. The content of the payment order shall not be altered and the Bank shall arrange the performance of the altered payment order within the same or shorter period of time than the time would be needed for the performance of the payment order defined by the Client.

The Bank shall not be liable for any damages arising from situations where the Client submits a given type of payment order to the Bank but the order – due to any legislative provision or rule applied by international payment systems – may only be executed through another type of payment order (this refers to the possibility of executing orders in general or by the time required), and while modifying the type of the payment order the content of the order is altered due to the features of the payment system to be applied. The Bank is entitled to modify such payment orders in a way to make it possible to execute them; modification shall only take place in the interest of the Client's payment order to be executed.

- 4.8. Orders shall be submitted by the Client to the Bank during such hours and on such dates that leaves the Bank sufficient time to execute them. Unless proven to the contrary, the receipt, and the time of receipt (year, month, day, hour, minute) of any order, notice or other document sent to the Bank shall be certified by the data printed on the document by the Bank's time stamping system. The placing of an order in the Bank's post-box does not mean that it has been received by the Bank. With respect to orders sent electronically, the time of receipt shall be the electronic time of receipt registered and recorded by the Bank's IT system.
- 4.9. If the Client requires the order to be executed at a particular future time or wishes it to be executed in a manner that differs from the usual practice, he must draw the attention of the Bank to this on the order. The Client shall be liable for any potential extra costs incurred due to this, as well as for any damages arising from any failure to indicate such requirements in advance.
- 4.10. The Bank shall consider any order to be fulfilled on a given date and received by the Bank before the due date (standing order, order with value date) as an order received earlier than the ones received and to be executed on the given due date.
- 4.11. In the prevailing List of Conditions, the Bank shall specify the cut-off time within the Bank Business Day – for each type of transaction – up to which the Bank shall perform its tasks relating to the fulfilment of received orders with no specification of a later value date on the given day. After this time, the Bank shall consider any orders with no specification of a later value date received on the given day as arrived on the Bank Business Day following the day in question, except the cases described in section 4.8. and instant transfer orders. The

cut-off time for execution of instant transfer orders is 24:00 every calendar day. Orders with the specification of a later value date shall be considered to be received on the value date and the Bank shall perform its tasks deriving from the order on the value date previously to the non-advantageously ranking orders received on the given date.

- 4.12. The Bank shall only start and perform the processing of the Client's orders by the deadline specified in its List of Conditions if all data necessary for such performance – including identification of the persons with rights of disposition – as well as the financial coverage necessary are available to the Bank. Deadlines specified in the List of Conditions shall only be adhered to by the Bank if payment orders are completed with correct and accurate data, and require no separate handling. The Bank reserves the right to make any corrections if according to its judgment it is possible to complete the missing data based on the ones provided on the order, but as a result, the parties may consider as if the payment order was received on the next Bank Business Day, or the Bank may refuse to execute the order without any consideration. The Bank shall inform the Client of such rejection. The Bank may perform partial execution if only a part of the necessary coverage is available, should a legislative provision so require. The Client understands that if there is a lack of funds, the Bank shall put the order(s) on hold and place it/them in a queue – except for instant transfer orders. If, on the first Bank Business Day following the submission and/or value date of the order(s) uncovered, the funds are made available, the Bank shall perform the transfer(s) that are on hold prior to executing the transfer orders that arrive on that day. If the required funds are still not available, the Bank shall – unless prohibited by a provision of the law – may delete the transfer orders on hold within 3 Bank Business Days calculated from the original receiving and/or value date. The Bank shall accept no liability for any damages arising from such procedure. If the fulfilment of the order is prevented by any other obstacle, the Bank shall inform the Client about this.

Conversion

- 4.13. If the processing of the order requires conversion between different currencies, and if, following launching of the conversion process, the order cannot be executed due to a lack of data, the Bank shall be entitled to keep the funds originating from the conversion on a non-interest-bearing suspense account until it receives the missing information from the Client, or an order for the item to be cancelled. Any damage arising from late fulfilment due to the need to supplement the data, or from any exchange loss resulting from cancellation, shall be borne by the Client.

4.14. In case of orders requiring conversion, submitted in a currency different from the currency of the account, the Bank is blocking on the Payment account until the debiting of the account a maximally 4% extra coverage in excess of the counter-value of the amount of the order converted to the currency of the account to be debited, in order to cover eventual changes in exchange rates. The Bank calculates the coverage amount and on basis of that the blocking at the exchange rate applicable on the day previous to the processing day of the payment order set forth in the List of Conditions. The debiting of the transaction shall take place on the day according to the List of Conditions, at the exchange rate actually posted by the Bank, and at the same time the blocked amount will be released. If the appropriate financial coverage including the extra coverage necessary according to the present section, is not available on the account to be debited on basis of the payment order, the Bank is henceforth treating the order as an uncovered order according to section 4.12. of present General Terms and Conditions. The Client and the Bank agree that if it would be necessary due to exchange rate changes arising from actual financial processes, the Bank is entitled to request extra coverage in excess of the 4% measure. The Bank undertakes no liability for damages arising from the blocking of the extra coverage due to eventual changes in exchange rates respectively from the treatment of the order as uncovered order as specified in this point.

Withdrawal and modification of orders

4.15. The client may neither withdraw nor modify payment orders following their receipt by the Bank. Any request for withdrawal or modification sent by the Client shall be examined by the Bank making every effort to fulfil the Client's request for withdrawal or modification. If the Client also determined a debit date, he/she shall be entitled to withdraw the payment order by the Bank Business Day immediately preceding the debit date, by the cut-off date of the Bank Business Day as specified in the List of Conditions for the given order type. In the case of payment orders initiated by or through the beneficiary, the withdrawal of the payment order requires the consent of the beneficiary.

4.16. The Client shall provide the Bank with instructions relating to the withdrawal or modification of submitted orders in writing or through the telephone or electronic bank service. Instructions submitted for the withdrawal or modification of orders shall be clearly indicated as such. In the event of withdrawal or modification of an order, the Bank shall be entitled to charge a separate fee, as specified in the List of Conditions.

4.17. In the case of withdrawal or modification instructions received according to section 4.14, the Bank shall perform the reverse booking of the executed order, and regard the reversal as having been carried out, only as soon as it receives approval and confirmation from the third party concerned (i.e. the beneficiary and/or the recipient bank) and after the counter-value of the cancelled order was transferred back to the Bank. All costs associated with the withdrawal or modification of the order shall be borne by the Client. In the case of withdrawal or modification of a foreign currency transfer order given by the Client to the Bank, the Client shall bear the related exchange risk. The Bank shall accept no liability for any damage arising in relation to the withdrawal or modification. In the event of withdrawal or modification of an order, the Bank shall be entitled to charge a separate fee, as specified in the List of Conditions.

Exchange rates

4.18. Unless otherwise agreed, orders received to be processed and executed on the same day and requiring conversion shall be executed by the Bank using the foreign exchange buying/selling rate posted by the Bank at latest by 3.00 pm, listed on the basis of market processes of the given day. The Bank shall perform conversion through HUF, that is, when performing conversion between two different currencies, it applies the buying rate for the currency of the order and the selling rate for the currency of execution. Daily exchange rates applied according to this section shall be published by the Bank every day in a so-called table of exchange rates on the website www.unicreditbank.hu and in its branches. If the Client agreed upon a special exchange rate with the Bank for a given payment transaction requiring conversion, in relation to which the Client submits a special order for FX transfer between accounts, the Client shall refer to the transaction with special exchange rate in the respective field of the order, in the manner required by the Bank. Any extra costs incurred or damage arising from any omission to do so, or due to any wrong reference made on the order to any transaction with special exchange rate without being entitled to such rates, shall be borne by the Client. The Bank reserves the right to apply the rate effective by the time of processing of the order or – subject to the value of the order exceeds the value specified in the List of Conditions – a single rate derived from the market rates subject to the following conditions: there is a significant difference between the Bank's quotation and the market rate due to the actual market rate changes and the order is submitted during the period set out in the List of Conditions.

Rejection of orders by the Bank

- 4.19. The Bank shall refuse to execute any order that conflicts with any provision of the law.
- 4.20. The Bank shall compensate the Client for any damage arising from the late or erroneous execution of payment orders or from the erroneous debiting of the Payment account if the damage occurred for reasons imputable to the Bank. The Bank is entitled to correct any credit or debit entry made by it in error without any instruction of the Client to this effect. For wrong entries made through the Bank's fault, no commission shall be charged.
- 4.21. The data or instructions indicated in the "Notes" ("Közlemény") section of the order slips are only intended for the beneficiary of the payment; they do not affect the Bank's rights or obligations, and the Bank does not check their accuracy. The Bank shall solely check the fields on the payment order those are compulsory to be checked by the virtue of law.
- 4.22. The Bank accepts from its Client keeping a Payment account with the Bank and also from Clients keeping no Payment account with the Bank cash payments for paying customs duties (customs and non Community tax) and for fulfilling customs duty deposit according to the Bank's rules related to payments at the cash desk. The payment of customs duty in cash shall be considered fulfilled on the day when the amount paid is credited to the public account of the all-time Hungarian tax authority. In order to certify the payment of customs duty, the Bank forwards the customs authorities the data of the cash payment order as well as of any other payment order submitted by clients for the purpose of paying customs duty against payment of a special fee defined in the prevailing List of Conditions; regarding the forwarding of data to customs authorities, the Client giving such orders releases the Bank from the obligation to keep bank secret.

5. Date and place of performance

- 5.1. The place of performance of payment obligations arising in the course of relations between the Bank and the Client shall be the organizational unit of the Bank which the Client concluded an agreement with or which is providing the given financial/supplementary financial service, or the account management institution where the Bank maintains its own account.
- 5.2. The time of performance of any payment made in the Bank's favour – if the Client's Payment Account is maintained by the Bank – is the day when the Bank

debits the Client's Payment Account, otherwise the day when the amount is credited to the Bank's account or to another Payment Account designated by the Bank; in case of cash payments, the day when the cash amount is deposited at the cash desk of the Bank, and in the case of amounts paid at a post office, the day when the amount is credited to the Bank's account.

- 5.3. The time of performance of the Bank's payment obligations towards the Client is the day when the Bank's account is debited or, if the Client keeps its bank Payment Account with the Bank, the day when the amount is credited to the Client's Payment Account.
- 5.4. The Bank shall fulfil the tasks deriving from the execution of payment orders by the time (Value Date) defined in the effective provisions of law on cash transactions, and in the provisions of the Bank's List of Conditions.
- 5.5. The Client understands that, in the course of performing foreign exchange transactions, the Bank takes into account the bank holidays of the various countries involved. If the expiration date of a loan or deposit as defined in the agreement, or the due date of any costs or fees falls on a Bank Holiday, then – unless the agreement between the Parties provides otherwise – the Bank shall regard the first Bank Business Day following the Bank Holiday as the due date, unless the Bank Holiday falls on the last day of the month, since in the latter case – in the absence of a provision to the contrary in the agreement, and not including the charges referred to in section I.2.5. – the last Bank Business Day preceding the Bank Holiday shall be the due date.

The maturity of payments related to credit/loan agreements of private customers shall be governed by the provisions of the General Business Conditions for Private Customers and the Bank Card Terms and Conditions.

6. Bank secret, management of personal data, data supply to third parties

- 6.1. Bank secret shall mean any fact, information, solution or data that relate to the identity, data, financial position, business activity, management, ownership structure and business relations of the Client, as well as to the balance and activity of his/her Payment account managed by the Bank or to his/her agreements concluded with the Bank. Regarding the provisions on bank secrets persons should be deemed as Clients who wish to use any financial services, additional financial services, investment

services provided by the Bank and contact the bank for this purpose, but does not use these services.

- 6.2. Bank secrets may only be disclosed to a third person in the cases and under the conditions specified in the prevailing provisions of Hpt.
- 6.3. 5.3 Pursuant to the provisions of CCIS Act, credit institutions (as reference data providers) are obliged to join the Central Credit Information System and supply data as stipulated in the CCIS Act. Furthermore, the Bank as Reference Data Provider shall supply the Reference Data handled by it immediately to the financial enterprise managing the CCIS, and shall do so with respect to any modification of Reference Data already supplied.
- 6.4. The Bank has an obligation to supply information:
 - 6.4.1. For **natural persons** in the following cases:
 - 6.4.1.1. subsequently to signing the Agreement subject to data supply, and the modification of the registered reference data (standard obligation for data supply),
 - 6.4.1.2. with regard to data concerning the amount and currency of the capital debt of the Client, by the fifth banking day of the month following month under review to the financial enterprise handling CCIS, and if the Client
 - 6.4.1.3. provides false information or uses counterfeit or forged documents when entering into a loan/ credit agreement, or initiating the conclusion of an agreement for financial leasing, the provision of payment services, the issuance of electronic money or non-cash payment instruments and the provisions of related services, undertaking of guarantees or bank guarantees or any other banker's obligations, or the provision of investment loan or securities lending, and this may be proved by documents,
 - 6.4.1.4. or the use of this serves as basis for the Court's final decision to establish a criminal offense as defined in Art. 274-277 of Act IV of 1978 on the Penal Code, or in Art. 342., 343., 345. or 346 of Act C of 2012 on the Penal Code.
 - 6.4.1.5. fails to meet his/her payment obligations provided for under the Agreement subject to data supply, and the amount being unpaid and overdue exceeds the monthly minimum wage applicable at the time of such payment becoming overdue, and such default exceeding the amount of minimum

wage lasts more than ninety days in a row. For the same natural person, the breach of agreement has to be considered separately for each legal relationship if several legal relationships exist at the same time,

- 6.4.1.6. if the court, as a result of the Client using a non-cash payment instrument, establishes by a final judgment that the Client has committed a crime as defined under Article 313/C of the Act IV of 1978 on the Penal Code or in Art. 374. Section 5 and Art. 393. of Act C of 2012 on the Penal Code.
- 6.4.1.7. The Bank is obliged to supply the data within five days in the cases listed in section 6.4.1.1. and 6.4.1.3 – 6.4.1.6, and the start date of deadline calculation shall be:
 - 6.4.1.7.1. the date of signing the Agreement subject to data supply in the case referred to in section 6.4.1.1.
 - 6.4.1.7.2. the expiration of the time set forth in section 6.4.1.5.
 - 6.4.1.7.3. the availability of the document proof in the case listed in section 6.4.1.3.
 - 6.4.1.7.4. the time of acquiring knowledge of the final court decision in the cases referred to in sections 6.4.1.4. and 6.3.1.6.
- 6.4.2. For **enterprises** in the following cases:
 - 6.4.2.1. subsequently to signing the Agreement subject to data supply, and the modification of the registered reference data (standard obligation for data supply),
 - 6.4.2.2. with regard to data concerning the amount and currency of the capital debt of the Client, by the fifth banking day of the month following month under review to the financial enterprise handling CCIS, and fails to fulfil the payment obligations undertaken in the Agreement subject to data supply when the overdue, not yet paid debt remains outstanding for more than 30 days.
if the Client
 - 6.4.2.3. fails to perform its payment obligation according to an Agreement subject to the data supply and the unpaid and overdue debt exists for a period exceeding thirty days.
 - 6.4.2.4. is in breach because a claim in the amount of more than one million Hungarian forints is registered against the Client's payment account due to the lack of funds for a period exceeding thirty days.

6.4.2.5. is in breach of any obligation undertaken in an agreement concerning the acceptance of non-cash payment instruments, and if due to this reason such agreement was suspended or terminated., and

6.4.2.6. The Bank is obliged to supply the data within five days in the cases listed in section 6.4.2.1. and 6.4.2.3 – 6.4.2.5, and the start date of deadline calculation shall be:

6.4.2.6.1. the date of signing of the Agreement subject to data supply in the case referred to in section 6.4.2.1.

6.4.2.6.2. the expiration of the time set forth in section 6.4.2.3., 6.4.2.4.

6.4.2.6.3. the availability of the document proof in the case listed in section 6.4.2.5.

6.5. The Bank's obligation to provide notifications:

6.5.1. In the cases outlined in sections 6.4.1.1., 6.4.1.3.–6.4.1.6 and 6.4.2.1., and 6.4.2.3.–6.4.2.5. the Bank informs the Client of the handover taking place within a maximum of five banking days of the handover to the financial enterprise handling CCIS.

The Bank shall obtain the written consent of the natural person Client regarding his/her details being taken over from the CCIS by a different reference data supplier prior to handing over the reference data to the CCIS. This consent may be provided by the natural person Client at any time during the period when the data is registered in the CCIS. The Client's consent is not necessary for taking over data handed over and managed on the basis of sections 6.4.1.3-6.4.1.6. If the Client will not consent to his/her data being taken over from the CCIS, the CCIS will only contain the following data:

6.5.1.1. date and place of the statement

6.5.1.2. identification details of the reference data supplier

6.5.1.3. identification details of the Client

6.5.1.4. a comment containing the refusal of consent.

The natural person Client's written statement giving or refusing consent is applicable to the Client's every Agreement subject to data supply. If the Client changes the contents of the written consent, or withdraws or grants his/her consent regarding the Agreements subject to data supply at a later date, in all cases the natural person's latest written statement shall prevail in all his/her Agreements subject to data supply.

During the preparation of the Agreement subject to data supply, prior to signing the agreement, the Bank informs the natural person handling the matter in writing about the prevailing rules regarding CCIS, about the aim of the register,

the rights of the person whose data is registered, the fact that data handled by CCIS may only be used for purposes defined by law, about the fact that his/her details will be handed over in circumstances defined in Agreement 6.4.1.1. and 6.4.2.1., as well as that they may be handed over in circumstances defined in sections 6.4.1.3 – 6.4.1.6.

30 days before the scheduled data handover according to section 6.4.1.5, the Bank informs the natural person about the fact that his/her reference details as defined in Agreement 6.5.2.1.1.-6.5.2.22 will be entered into the CCIS unless he/she fulfils her obligations laid down in the agreement. At the time of the signing of the agreement, the natural person certifies by his/her signature that he/she understands the information he/she received regarding this matter.

Prior to signing the agreement, the Bank is duty bound to inform enterprises in writing that in circumstances defined in Sections 6.4.2.2.-6.4.2.4., the reference data might be entered into the CCIS. This information must indicate the purpose of handing over the data, the type of data being handed over, and it must state the fact that after the data is entered into the CCIS, the financial enterprise handling the reference data may pass the reference data to other reference data suppliers for purposes defined in the CCIS Act.

6.5.2. Information that must be supplied to and registered by the Central Credit Information System after January 1, 2006 or April 1, 2006:

6.5.2.1. regarding natural persons:

6.5.2.1.1. Name

6.5.2.1.2. Name at birth

6.5.2.1.3. Date and place of birth

6.5.2.1.4. 6.5.2.1.4. Mother's maiden name

6.5.2.1.5. ID or passport number or the number of any identification document suitable for certifying personal identity (according to Act LXVI of 1992 on the registration of personal data and addresses of citizens),

6.5.2.1.6. Address

6.5.2.1.7. Mailing address

6.5.2.1.8. electronic mailing address

Data of the Agreement subject to data supply:

6.5.2.1.9. the type and identification number of the agreement,

6.5.2.1.10. the date of the signing, expiration and termination of the agreement,

6.5.2.1.11. the type of client (debtor, co-debtor),

6.5.2.1.12. the agreement amount

6.5.2.1.13. the amount and the currency of the instalment of the contractual amount,

- 6.5.2.1.14. the method and frequency of the payment of instalments,
- 6.5.2.1.15. the date on which the conditions described in Section 6.4.1.4. subsist,
- 6.5.2.1.16. the amounts overdue and not yet paid when the conditions described in Section 6.4.1.4. subsisted,
- 6.5.2.1.17. the method and termination date of the overdue and not yet paid debt,
- 6.5.2.1.18. notes regarding transfer of the claims to another reference data supplier, notes referring to any litigation,
- 6.5.2.1.19. prepayment,
- 6.5.2.1.20. date of prepayment,
- 6.5.2.1.21. the prepaid amount and the amount and currency of the outstanding capital debt,
- 6.5.2.1.22. the amount and currency of the outstanding capital debt,
- 6.5.2.1.23. 6.5.2.1.23. the date and grounds for the rejection of the application,
- 6.5.2.1.24. documents used for evidence,
- 6.5.2.1.25. the number of the final court ruling,
- 6.5.2.1.26. the name of the court acting in the case,
- 6.5.2.1.27. the contents of the operative part of the ruling,

Data regarding the use of no cash payment instruments:

- 6.5.2.1.28. the type and number of the no cash payment instrument,
- 6.5.2.1.29. the time of cancellation,
- 6.5.2.1.30. the time, number and amount of the transaction carried out with the cancelled no cash payment instrument,
- 6.5.2.1.31. the number of unauthorized uses,
- 6.5.2.1.32. the amount of damages,
- 6.5.2.1.33. the time of the finalisation of the court ruling,
- 6.5.2.1.34. notes referring to any litigation.

6.5.2.2. Information that can be registered regarding enterprises:

Identification data:

- 6.5.2.2.1. company name, name
- 6.5.2.2.2. registered seat
- 6.5.2.2.3. tax number
- 6.5.2.2.4. registration number, number of the private entrepreneur's entrepreneur ID

The details of the agreement subject to data supply:

- 6.5.2.2.5. the type and identification number of the agreement,
- 6.5.2.2.6. the date of the signing, expiration and termination of the agreement,
- 6.5.2.2.7. the method of the termination of the agreement,
- 6.5.2.2.8. the contractual amount and currency,
- 6.5.2.2.9. the amount and the currency of the instalment of the contractual amount,

- 6.5.2.2.10. the method and frequency of the payment of instalments,
- 6.5.2.2.11. the date on which the conditions described in Section 6.4.2.3. subsist,
- 6.5.2.2.12. the amounts overdue and unpaid when the conditions described in Section 6.4.2.4. subsisted,
- 6.5.2.2.13. the due date and amount of the overdue and unpaid debt,
- 6.5.2.2.14. the method and termination date of the overdue and unpaid debt,
- 6.5.2.2.15. notes regarding transfer of receivables to another reference data supplier, notes referring to any litigation,
- 6.5.2.2.16. fact of prepayment,
- 6.5.2.2.17. date of prepayment,
- 6.5.2.2.18. the prepaid amount and the amount and currency of the outstanding capital debt,
- 6.5.2.2.19. the amount and currency of the outstanding capital debt,

Data regarding accounts where spooled claims are registered:

- 6.5.2.2.20. the number of the agreement regarding the opening of the account,
- 6.5.2.2.21. the amount and currency of the spooled claims,
- 6.5.2.2.22. the start and end date of the spooling of the claims,
- 6.5.2.2.23. notes on any litigation.

Data regarding agreements on the acceptance of no cash payment instruments:

- 6.5.2.2.24. the date of the signing, expiration and termination of the agreement,
 - 6.5.2.2.25. notes on any litigation.
- 6.6. Request for information by the Client concerning data entered in the Central Credit Information System**

6.6.1. Anyone is entitled to request information of any reference data provider on their data registered in the CCIS and on the reference data provider having supplied those data.

6.6.2. Those registered in the CCIS are entitled to unlimited access to their own data and information regarding who accessed the data, when, and on what grounds; therefore, no costs or other fees may be charged.

6.6.3. The reference data provider shall forward the request of the client referred to in section 6.6.2. immediately, but latest within two banking days to the financial enterprise handling CCIS, which shall send the requested data:

- a) enclosed to the reference data provider within three days, or

- b) upon request of the client via electronic data communication to the electronic mail address specified by the client in its request. In case of sub section a) the reference data provider shall send the data immediately, but latest within two banking days as of receipt to the Client enclosed, posted with delivery note.

6.7. Management and deletion of reference data by the CCIS

6.7.1. The financial enterprise managing the CCIS shall handle the reference data subject to data handover as described in Sections 6.4.1.1. deletes the data permanently, in an irretrievable manner within one working day of the termination of the agreement. The financial enterprise managing the CCIS shall handle the data listed in Section 6.4.2.1. and permanently delete it after 5 years from the date described in Section 6.7.5.

6.7.2. At the time signing the Agreements subject to data supply, the Bank informs in writing the natural person signing the agreement about the possibility that the financial enterprise managing the CCIS may handle the data following the termination of the agreement, at the request of the natural person. At the time of signing the agreement or during the agreement's validity, the registered natural person may request in writing the financial enterprise managing the CCIS, through the reference data supplier, to handle his/her data for up to five years following the termination of the agreement. The consent to data handling after the termination of the agreement may be withdrawn in writing at any time. This is done through the reference data supplier while the agreement is valid and directly through the financial enterprise managing the CCIS after the termination of the agreement.

6.7.3. Prior to signing the agreement subject to data supply, in order to foster informed decision-making, the Bank informs the natural person of the data taken over from the CCIS, and the Bank's conclusions based on the data regarding the natural person's creditworthiness, and if necessary, informs the natural person about the risks of taking out loans.

6.7.4. The financial enterprise managing the CCIS handles the reference data for five years from the date determined in section 6.7.5. Following the expiration of five years, or if the natural person withdraws his/her consent for the further handling

of the data in accordance with Section 6.7.2., the financial enterprise managing the CCIS deletes the data permanently, in an irretrievable manner.

6.7.5. The start date of calculation of the period defined in section 6.7.4.:

- a) in cases described in Sections 6.4.1.5. and 6.4.2.3., if the debt is still outstanding, the end of the fifth year from the date of the data supply ,
- b) the date of supplying data in the cases described in sections 6.4.1.3., 6.4.1.4. 6.4.1.6. and 6.4.2.5
- c) the last day of the spooling of claims in case of 6.4.2.4.,
- d) for enterprises, the date of termination of the contract.

6.7.6. The financial enterprise managing the CCIS shall immediately and definitively delete the reference data if the reference data supplier cannot be determined, or if he/she learns that the reference data were entered to the CCIS unlawfully.

6.7.7. The financial enterprise managing the CCIS deletes the reference data supplied in accordance with Section 6.4.1.5. permanently, in an irretrievable manner without delay, one year after the payment of the overdue outstanding debt in the case of the payment of outstanding debts that arose from agreements subject to data supply.

6.8. Legal remedies, objections and recourse to legal action by the Client

6.8.1. The Client may object to the supply of its reference data to the financial enterprise managing the CCIS, or to the manner of handling of such data by the financial enterprise managing the CCIS, and may request the correction or deletion of the reference data, by submitting such written request to the reference data provider supplying the reference data to the financial enterprise managing the CCIS, or to the financial enterprise managing the CCIS.

6.8.2. The financial enterprise managing the CCIS is duty bound to send the Complaint within two working days of its receipt – while also informing the registered person – to the reference data supplier who supplied the reference data subject to the Complaint to the financial enterprise managing the CCIS, except if the reference data supplier was terminated without a legal successor, and the claim resulting from the Agreement subject to data supply has not been transferred to another reference data supplier, or the person of the reference data supplier is cannot be determined.

- 6.8.3. If the reference data provider accepts the objection, it shall supply the reference data to be corrected or deleted immediately but within five working days at the latest – by notifying the Client of this fact at the same time – to the financial enterprise managing the CCIS, which shall register such changes immediately, but within two working days as of the closing of the enquiry at the latest.
- 6.8.4. The financial enterprise managing the CCIS register the changes immediately, but within five working days at the latest even if the reference data provider has ceased to exist without succession and the claim arising from the Agreement subject to data supply has not been transferred to any other reference data provider, or if the identity of the reference data provider cannot be established and so the objection submitted was examined.
- 6.8.5. The financial enterprise managing the CCIS shall provide notification on such correction or deletion immediately, but within two working days at the latest to all reference data providers which have requested reference data during the year preceding the correction or deletion on the registered entity.
- 6.8.6. The Client may bring an action against the reference data provider or the financial enterprise managing the CCIS due to the unlawful supply or management of his/her recorded reference data, or the correction or deletion thereof.
- 6.8.7. The statement of claim shall be submitted to or sent by registered post to the competent district court having jurisdiction where the Client is domiciled within thirty days upon receipt of the information on the examination of the objection. If such deadline is missed, the Client's justification for the delay may be accepted.
- 6.8.8. The Client may also bring an action if the reference data provider or the financial enterprise managing the CCIS fail to meet their notification obligations defined in CCIS Act. In such cases, the timeframe available for submission of the statement of claim shall be calculated from the date of expiration of the deadline set for the notification to be given.
- 6.9. Pursuant to the Hpt., the transfer of data by the Bank to a foreign financial institution shall not constitute a breach of bank secrets if the Client (the data subject) has given his/her written consent to this and if, at the foreign financial institution (data manager), the conditions for data handling satisfying the requirements set by Hungarian law are met with respect to each item of data, and if the state in which the foreign financial institution is seated has statutory regulations on privacy that satisfy the requirements set by Hungarian law.
- 6.10. According to Hpt. the disclosure by the financial institution to an intermediary being in contractual relationship with the financial institution of data pertaining to the fulfilment of the contract relating to financial services intermediated by the intermediary shall not constitute a breach of bank secrecy. On the basis of that, if the contract entered into between the Client and the Bank on financial services or activities auxiliary to financial services has been established by involvement of an intermediary and the Client has breached the contract – especially if the Client has not duly performed its payment obligations to the Bank – the Bank is entitled to inform the intermediary on basis of Section 164 Subsection q) of Hpt by providing data pertaining to the performance of the contract on financial services intermediated by the intermediary in order to enable the Client to contact the Bank either in writing, by telephone or personally, to re-establish the due fulfilment of the contract.
- 6.10/A. The Bank and the financial institutions, payment institutions, electronic money institutions, investment firms, insurance companies, AIFMs and UCITS managers they control shall be allowed to exchange the personal data of clients they process, data classified as bank secrets, securities secrets, payment secrets and insurance secrets, and data classified as business secrets to the extent required in connection with their operations and for the provision of their services the data processors participating in such shared data processing, shall be permitted to transmit such data directly with a view to allowing access to their individual services, and to process the data thus received during the time period for setting up and during the existence of client relationships.
- With regard to the Bank and other companies controlled by it, accessing and processing the data referred to above shall be allowed only to companies
- a) such that are pursuing activities:
 - aa) aiming to promote non-cash digital payment services and to provide consumers with such payment methods,
 - ab) aiming to introduce digital applications to support the management of parties who are not consumers,

ac) ac) working to improve the financial awareness of consumers and to introduce digital financial means to them, and data processing is performed in the interest of setting up client relations in that context of services.

6.11. The Bank is entitled to record images, using video and photographic equipment, of the individuals and Clients entering its premises, and to store and use such images exclusively for security purposes. Without the client's consent, the Bank shall not make the pictures or voice recordings public, except in cases specified by law.

6.12. Provision of data by the Client is voluntary, except in the cases mentioned in this section. In some cases, the information to be provided by the Client is stipulated by law, including the Credit Institutions Act, the AML Act, Act CXX of 2001 (Capital Market Act), the Investment Services Act, and Government and Ministerial decrees issued on the basis of the mandate in these laws.

Only the Bank and the persons to whom the Bank legally transmits the data is entitled to handle and process Client's personal data. The Bank only processes the personal data provided by the Client until this is required to fulfill its obligations and to exercise its rights stipulated by law.

The Client shall – within the limits permitted by the General Data Protection Regulation – have the right to request from the Bank information on the processing, rectification or erasure – except for data processing stipulated by law – of personal data or restriction of processing of personal data concerning him or her or to object to processing his or her data. Client shall also have the right to data access and to data portability. The Bank shall respond to the Client's request within one month, in writing. This deadline may be extended by two further months, where necessary, and the Bank shall inform the Client of any such extension within one month of receipt of the request, together with the reasons for the delay.

6.12/A. The Bank has a data protection officer.

6.12/B. The Client may apply to the National Data Protection and Freedom of Information Authority or to the court in the case of violation of his/her rights attached to the management of his/her personal data.

6.13. The Bank shall ensure that the entities to which it supplies data handle such data in compliance with legislative provisions concerning bank and securities secret as well as the prevailing legislation on privacy.

6.14. The Client is entitled to give instructions at any time in order not to be directly contacted by the Bank for direct marketing purposes. Such instructions may be given in person at any branch, or – in a manner allowing for his/her personal identification – by a letter sent to the Bank's registered seat, or by e-mail to leiratkozas@unicreditgroup.hu.

6.15. In line with Section 276 (3) of the Credit Institutions Act, the Bank defines the rules of personal data processing in these General Terms and Conditions. Detailed information on data processing, in compliance with the General Data Protection Regulation, related to a contract to be concluded with a natural-person client and to the contractual relationship is contained in Annex 2 that constitutes an inseparable part of these General Terms and Conditions.

7. The Bank's liability

7.1. If the Bank receives and forwards documents based on the order of the Client, it shall verify them only in terms of whether they are consistent with the order. The Bank shall not, however, be liable for the authenticity, validity and content of such documents.

7.2. The Bank shall effect payments and deliver documents to any person only if it deems, as per the inspection of documents and based on the order and/or legislative provisions, to be authorized to receive the payment or the documents.

7.3. The Bank shall check, with a level of care that may be expected of a financial institution, the documents presented for the purpose of proving a person's identity, right of representation or authorization. The Bank shall accept no liability for the authenticity of such documents, nor for their being forged or counterfeit if it cannot be ascertained by careful inspection.

7.4. If the Bank has serious doubts regarding the authenticity or validity of the order, it shall be entitled to refuse the order without any reason. The Bank shall accept no liability for any damages arising from the refusal of the order. The Bank shall not be liable for any damages arising from the fulfilment of any order whose false or forged nature could not be ascertained by the careful inspection that may be expected.

7.5. The Bank shall not be liable for any damages arising from force majeure, domestic or foreign legislation or measures taken by any domestic or foreign authority out of the Bank's sphere of interest.

- 7.5/A. The Client acknowledges that – upon restrictive provisions of law, international organizations or authorities or provisions followed or to be followed by the Bank – Bank shall refuse to execute payment orders or require further information and documents for examining the possibilities of executing payment orders. The Bank shall not be liable in the event when a payment order cannot be executed by reasons beyond the control of the Bank (e.g. mandatory sanctions imposed on the Bank or other intermediary financial institutions). The Bank shall accept no liability for any damages arising from such refused or failed payment orders. The Bank shall inform the Client without delay about any payment order refused by the specified means of communication.
- 7.6. Should the Bank have to translate documents received or forwarded based on the Client's instructions, or have to interpret a document drawn up according to the laws of a foreign state, it shall not be held liable for any damages originating from this. The Client shall bear the costs of translation.

8. Use of agents

- 8.1. The Bank is entitled to avail of the services of a third party if necessary in order to perform an order received from the Client. The Bank shall not be responsible for the actions and omissions of the third party if such action or omission occurred as a result of unforeseen circumstances beyond the control of the third party. Unless otherwise agreed by the parties, costs charged to the Bank by such third persons shall be borne by the Client. Regarding the costs incurred in connection with engaging such third persons, the Bank may only provide information to the extent that it is in possession of such information. The Bank shall not be liable for the selection, involvement or omission of the third person if such person was assigned upon the Client's instructions or based on any legislative provision. In case of Clients which do not qualify a consumer, if the liability of the third party involved is limited by law or by the contract between the Bank and the third party, the Bank's liability shall be adjusted accordingly. If, during the performance of the contract, the Bank avails of the services of a foreign bank, financial institution or settlement agent (e.g. VISA International, correspondent bank, clearing house), the performance in conformity with contract shall be governed by international agreements and regulations (customs). The Bank reserves the right to unilaterally choose its correspondent bank.
- 8.2. The Bank is entitled to outsource any activities related to its business as well as any activities it is required to conduct under the law, which are aimed at data management, data processing or data storage, provided that all requirements in connection with privacy are adhered to. The scope of activities outsourced by the Bank and the unit performing them are contained in the inseparable Annex 1 of these Terms and Conditions, which the Bank is entitled to unilaterally modify in the case of any change in the outsourced activities or in the units performing them.
- 8.3. If the Bank uses the services of a data processor to perform its data controller's activities, then such data processor shall control personal data on behalf of the Bank. The data processor and any person acting under the authority of the Bank or of the processor, who has access to personal data, shall not process those data except on instructions from the Bank, unless required to do so by Union or Member State law.
- 8.4. The Bank shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the statutory requirements and ensure the protection of the rights of the data subject.
- 8.5. The processor shall not engage another processor without prior specific or general written authorisation of the Bank.
- 8.6. The Bank shall be liable for any damages caused to a data subject as a result of unlawful processing or by any breach of data security requirements, and, provided that the infringement has been established with legally binding effect, it shall pay compensation for damages (liability and/or restitution). The Bank shall also be liable for damage caused by the data processor whose services it is using. The Bank shall also bear liability for damages caused by a controller that is in a joint controller relationship with the Bank, in which case liability for damages caused may be shared between the Bank and the joint controller as regulated by the contract they have concluded.

9. Cooperation, information, notification

- 9.1. The Bank and the Client shall duly cooperate throughout their contract relationships, and in the course of this cooperation they shall inform each other without delay of any important facts relevant

to the banking transaction as well as of any changes therein, in particular, of any changes in their names, addresses, telephone numbers, representatives, owners, financial position or business situation, as well as of all other changes concerning their identity and legal status. Any damage arising from failure to meet these obligations shall be borne by the defaulting party. The Bank reserves the right to send such information to the Client in a written form, by post.

- 9.2. Both the Bank and the Client shall make their notices to each other, their orders and their agreements in writing, or shall confirm them in writing. Electronic letters sent to an electronic mailing address shall not be considered a written form, or written confirmation/ notification.
- 9.3. The Parties shall respond to any questions related to the transaction or addressed by one to the other within 15 days at the latest, and shall draw each other's attention to any errors or omissions.
- 9.4. The Bank shall send its notifications (Account Statements, Breakdowns of Costs) once they are printed, put in envelopes and posted by the Bank itself or by a third party engaged by the Bank to the postal address specified by the Client. The Bank is not obliged to send any documents and notices to the Client by registered post with or without return receipt requested. Failing proof to the contrary, sending shall be deemed to have been made if a copy of the original document (including a copy that can be printed out at any time from a computer) is in the Bank's possession, and if the signed delivery register, receipt or the Bank's records kept for this purpose proves it. Unless legislative provisions concerning postal delivery, the prevailing General Terms and Conditions for postal services of Magyar Posta Zrt., or the agreement between the Parties provide otherwise, unless proven to the contrary the Bank shall be entitled to consider the written notice delivered to the Client inside Hungary after 5 working days, within the European Union after 9 working days, in Europe but outside the European Union after 10 working days from posting, or outside of Europe after 21 working days from posting. With regard to notices affecting a wide range of Clients, the existence of just one copy as per the above shall be sufficient for the purpose of proving that the circular has been sent. If the Bank serves data substituting account statement on electronic way by the virtue of electronic connection with the Client, the Parties consider the time of arrival of the data to the Client as it is registered by the informatics system of the Bank. The Bank shall not be held liable if, due to any incorrectness or change in the name or address provided

by the Client, or for any other reason outside the Bank's control, the delivery is delayed or fails. If the Client is a client qualifying as consumer or micro-enterprise, the Bank shall send an Account Statement in a paper format once a month, and shall make available the Breakdown of Costs once a month to such a Client.

- 9.5. If an electronic connection exists between the Client and the Bank, data sent electronically shall substitute the Account Statement, but upon request of the Client the Bank shall provide the Client with a printed copy of the Account Statement, for which service the Bank shall be entitled to charge an additional fee. The Bank shall provide the Client with a printed copy of the Account Statement once in a year or at contract expiration without fee, cost or other payment obligation. If the Client qualifies as consumer or micro-enterprise, the Bank shall charge no fee, cost or other payment obligation for making available or delivering the Account Statement once in a month. If the Client does not qualify as consumer or micro-enterprise, the Bank shall charge no fee, cost or other payment obligation for making available or delivering the Account Statement once in a year.
- 9.6. Upon the Account Owner's request, as a separate service, the Bank shall send the Account Statement in several copies to the Account Owner against payment of an extra fee according to the prevailing List of Conditions. The Bank is entitled to post the Client's Account Statements to send to the same postal address in the same envelope.
- 9.7. In continuing contractual relationships – including especially but not exclusively bank account contracts, credit/loan agreements as well as contracts for deposits tied up on a recurrent basis – the Bank shall send the Client a clear and comprehensive statement (extract) in a written form that is easy to understand at least once a year, and within thirty days after the time of termination of the contract. The Client may request – at his own expense – a statement on individual transactions carried out in the previous five years. The Bank is required to send such statements in writing to the Client at the latest within ninety days.
 - 9.7.1. In the case of Customers qualifying as consumer, the Bank shall provide the Customers with a Fee Statement free of charge once a year, until 31 January following the calendar year in question. Upon special request of the Customers qualifying as consumer, the Bank shall make the Fee Statement available to the Customers once a year, free of charge in paper format. The provision of further Charge Statements shall be subject to the fees set forth in the Bank's effective List of Conditions.

- 9.7.2. The Fee Statement shall be made available in the same manner as the Statement of Account.
- 9.8. Upon the Client's written request and at the Client's risk, the Bank shall retain the correspondence and deliver mails at the Bank's premises. The legal consequences of the delivery shall become effective on the subsequent day after such retention (deposition), and the Bank is entitled to deem the notification as received by the Client.
- 9.9. If the Client chooses to use the Bank's post-box (c/o) service, the Bank shall place all notices in that box unless otherwise agreed. The Bank shall be entitled to regard the notice as having been received by the Client on the first Bank Business Day following placement of the notice in the Client's post-box.
- 9.10. The Client shall send his/her written notices to the Bank to the address where the Bank keeps the Client's account or, if the Bank does not keep any Payment account for the Client, to the address where the contract was concluded. Unless proven to the contrary, regarding the receipt of written notices sent by the Client, the Bank's records shall be used as evidence.
- 9.11. Bank information made available to the Client shall only serve the Client's purposes. The Bank does not allow copying of the information provided by it in any format, nor their forwarding without authorization.
- 9.12. The Parties agree that if the Client has specified a mobile phone number contact, the Bank may inform the Client about its next due claim or in case of non-performance about its overdue claims by sending an SMS to the given phone number. The Bank draws the Client's attention to and the Client takes notice of the risks inherent in SMS services, especially that the Bank shall not be liable if due to a reason outside the scope of interest of the Bank (among others failing to notify the Bank about the change of phone number provided to the Bank by the Client or by the Guarantor/Joint and several guarantor), any unauthorised third party becomes aware of any information being bank secret forwarded as SMS, and the payment obligations of the Client according to the contract establishing the payment obligation shall exist irrespective of an eventually erroneous SMS content or a non-delivery of an SMS.
- 9.13. If the natural person or legal entity or other entity taking joint and several guarantee/guarantee for the payment obligation has specified a mobile phone number contact the Bank may inform the Joint and Several Guarantor/Guarantor about the non-performance of the Client

and the amount of the insured claim at the time of the notification by sending an SMS to the provided phone number. The Parties Agree that if the SMS was sent certifiably to the mobile phone number provided by the Joint and Several Guarantor/Guarantor to the Bank, the Bank will assume that the Joint and Several Guarantor/Guarantor had received the information contained in the SMS. The Bank draws the attention of the Joint and Several Guarantor/Guarantor and the Client to the fact and the Joint and Several Guarantor/Guarantor and the Client takes notice of the fact that the Joint and Several Guarantor/Guarantor is obliged to notify the Bank immediately of the change of his/her mobile phone number according to point I.9.1. of the General Terms and Conditions. The Bank draws the attention of the Joint and Several Guarantor/Guarantor to the fact that the Joint and Several Guarantor/Guarantor is obliged to notify the Bank immediately of the change of his/her mobile phone number according to point I.9.1. of the General Terms and Conditions. The Bank furthermore draws the Joint and Several Guarantor's/Guarantor's/Client's attention to the fact and the Joint and Several Guarantor/Guarantor/Client takes notice of the risks inherent in SMS services, especially that the Bank shall not be liable if due to a reason(s) outside the scope of interest of the Bank (among others failing to notify the Bank of the change of phone number provided to the Bank by the Joint and several guarantor/Guarantor), any unauthorised third party becomes aware of any information being bank secret forwarded as SMS, and the payment obligations of the Joint and Several Guarantor/Guarantor according to the joint and several guarantee contract /guarantee agreement/ statement of guarantee establishing the aforementioned payment obligation shall exist irrespective of an eventually erroneous SMS content or a non-delivery of an SMS.

10. Verification of and objections to the Bank's notifications

- 10.1. The Client shall review the correctness and completeness of the Payment account statements, settlements of securities, deposit and yield reports, other settlements, notifications regarding the fulfilment of orders and information related to expected payments and remittances (hereinafter: Notifications) without delay, to check them continuously and to raise potential objections regarding these and the Bank's other notifications – including any unauthorized transaction observed – in writing or over the phone (+36 1 325 3200 or +36 20/30/70 325 3200) to the Bank within 8

days from receipt. If no such objection is raised within this time, the Client shall be deemed to have accepted the Notification as accurate.

- 10.2. Any damage caused by any failure, whether due to wilful misconduct or negligence, to perform the obligations mentioned in section I.10.1 shall be borne by the Client.

11. Complaint management

11.1. Rules of Complaints handling for natural persons

11.1.1. Within the meaning of this section I.11.1., Client shall mean any natural person (as well as his/her proxy holder) who gets in business contact with the Bank without concluding any contract with the Bank for financial services, supplementary financial services, investment services or supplementary investment services.

11.1.2. The Client may lodge a Complaint in person or in writing, in any branch office of the Bank, by mail addressed to the central address of the Bank (1054 Budapest, Szabadság tér 5-6.) or by e-mail to panasz@unicreditgroup.hu, or over the phone at the Telefonbank's phone numbers +36 1 325 3200 or +36 20/30/70 325 3200 or by fax to the +36 1 374 7838 fax number.

11.1.3. The legal representative acting on behalf of the Client shall attach its proxy given by the Client.

11.1.4. Complaints made in person shall be investigated by the Bank without delay, and remedied to the extent possible by an immediate action. If the Client does not agree with the immediate action or such action is not possible, the Bank shall inform the Client about the data identifying the Complaint and draw up a record of the Complaint. The Client shall inform the Client about the data identifying the Complaint and receive a copy of the record drawn up of the Complaint from the Bank. Based on the record, the Bank shall further proceed in accordance with the rules set out in these Terms and Conditions concerning written Complaints.

11.1.5. Complaints lodged using the phone number provided for Complaint management, as well as any relating communication between the Client and the Bank shall be voice recorded. Voice recordings shall be kept by the Bank for five years following recording, and within this timeframe the Bank shall make it available upon the

Client's request in the form of an audio recording, furthermore – depending on the Client's request - provides free of charge the authenticated transcript of the audio recording or the copy of the recording within 25 days. In case of a Complaint through phone – if its immediate investigation should not be possible or the Client should not agree with the arrangement – the Bank shall inform the Client about the data identifying the Complaint and prepare a minutes of the Complaint and send its copy with the Bank's answer as set out in clause 11.1.6. accordingly to the Client.

11.1.6. The Bank shall investigate the Client's written Complaint immediately, and inform the Client of the results of the all-inclusive investigation of the Complaint, its standpoint and actions regarding the Complaint together with an explanation in writing, by sending such response within 30 days from submission of the Complaint, or in case of complaints related to payment services within 15 working days to the address specified by the Client, or if explicitly requested by the Client, through its Internet Banking service or via the UniCredit Mobile application. If all elements of the payment service complaint cannot be answered within 15 working days for reasons outside of the Bank, the Bank will send a temporary reply to the Client, which includes the reasons for the delay in the matter and the deadline for the final response. However, the deadline for sending the final reply cannot be later than the 35th working day following the submission of the Complaint. While handling complaints the Bank shall make reasonable efforts under the circumstances to avoid a consumer dispute of financial nature.

11.1.7. Should the Client not agree with the result of investigation of his/her Complaint lodged, he/she shall be entitled to seek legal remedy through other forums. The Client may submit his/her Complaint or application for legal remedy to the following organizations, having in mind the subject matter and the competencies of the organizations listed below:

- Magyar Nemzeti Bank (National Bank of Hungary) (1013 Budapest, Krisztina krt. 39., central mailing address: 1534 Budapest BKKP Pf.: 777, any Kormányablak (government office) or via Ügyfélszolgálat (client gate) phone: +36 80 203 776, e-mail: ugyfelszolgalat@mnbb.hu)
- Gazdasági Versenyhivatal (Hungarian Competition Authority) (1054 Budapest, Alkotmány u. 5. mailing address: 1245 Budapest Pf.: 1036, phone: +36 1 472 8900)

- Pénzügyi Békéltető Testület (Financial Arbitration Board) (1013 Budapest, Krisztina krt. 39., mailing address: Financial Arbitration Board 1525 Budapest BKKP Pf.: 172, phone: +36 80 203 776, e-mail: ugyfelszolgalat@mnbb.hu).
- The Client may also assert his/her claim through civil law actions.

The Bank informs the Client that the Bank declares its submission to the arbitration procedure and – in the absence of negotiated settlement – accepts the decision of the Financial Arbitration Board as binding, if the value of the transaction being the basis of the subject of the legal dispute is maximally 3 million HUF and the amount claimed by the Client is maximally 1 million HUF.

If the Complaint is rejected by the Bank – depending on if according to the standpoint of the Bank the Complaint lodged was aimed to investigate the violation of the consumer protection provisions set out in Act CXXXIX of 2013 on the National Bank of Hungary, or settle legal disputes pertaining to contract conclusion, validity, legal impacts and termination, or to contract violation and the legal impacts thereof – the Bank shall inform the Client if he/she may seek legal remedy through the organisation listed in a), c), or d) above.

11.2. Rules of Complaint management for non-natural persons

11.2.1. Within the meaning of this section I.11.2, Client shall mean any legal entity or unincorporated business organization, other organization or authority (as well as their proxy holder) which get in business contact with the Bank without concluding any contract with the Bank for financial services, supplementary financial services, investment services or supplementary investment services.

11.2.2. The Client may lodge a Complaint in person or in writing, in any branch office of the Bank, by mail addressed to the central address of the Bank (1054 Budapest, Szabadság tér 5-6.) or by e-mail to panasz@unicreditgroup.hu, or over the phone at the Telefonbank's phone number +36 1 325 3200 or +36 20/30/70 325 3200 or by fax to the +36 1 374 7838 fax number. Complaints made in person shall be investigated by the Bank without delay, and remedied to the extent possible by an immediate action. If the Client does not

agree with the immediate action or the immediate action is not possible the Bank shall inform the Client about the data identifying the Complaint and prepare a minutes of the Complaint. The Bank shall hand over the copy of the minutes of the Complaint to the Client. The Bank's procedure based on the minutes shall be the same as the procedure set out to the written Complaint in this General Terms and Conditions. If the Client does not agree with the immediate action or such action is not possible, the Client may also lodge its Complaint in writing.

11.2.3. The Complaint received on the phone number established for the dealing with Complaints and the verbal communication in connection with it shall be recorded. The Bank shall keep the record for five years from the recording, and within this timeframe the Bank shall make it available upon the Client's request in the form of an audio recording, furthermore depending on the Client's request provides free of charge the authenticated transcript of the audio recording or the copy of the recording within 25 days. In case of a Complaint through phone – if its immediate investigation should not be possible or the Client should not agree with the arrangement – the Bank shall inform the Client about the data identifying the Complaint and prepare a minutes of the Complaint and send its copy with the Bank's answer as set out in clause 11.2.5. accordingly to the Client.

11.2.4. The legal representative acting on behalf of the Client shall attach its proxy given by the Client.

11.2.5. The Bank shall investigate the Client's written Complaint immediately, and inform the Client of the results of the all-inclusive investigation of the Complaint, its standpoint and actions regarding the Complaint together with an short explanation in writing, by sending such response within 30 days from submission of the Complaint, or in case of complaints related to payment services within 15 working days from receipt of the written Complaint to the address specified by the Client, or in case of small business clients if explicitly requested by the Client, through its Internet Banking service. If all elements of the payment service complaint can not be answered within 15 working days for reasons outside of the Bank, the Bank will send a temporary reply to the Client, which includes the reasons for the delay in the matter and the deadline for the final response. However, the deadline for sending the final reply can

not be later than the 35th working day following the submission of the Complaint.

- 11.2.6. Should the Client not agree with the result of investigation of his/her Complaint lodged, the Client may also assert his/her claim through civil law actions.

12. Interests, fees, commissions, costs, and rights of the Bank and the Client to offsetting

Interests, fees, commissions and costs

- 12.1. The types, prevailing rates, due dates and calculation methods for interests, commissions, fees and costs charged for the services provided by the Bank are determined in the contract concluded between the Client and the Bank, in the Business Regulations pertaining to the various transactions complementing the contract, in the Bank's applicable List of Conditions, or by the law.
- 12.2. The conditions of changing the interest rates, commissions, fees and other conditions determined in individual contracts may be included in the contract, in the business regulations pertaining to the various transactions complementing the contract, in the List of Conditions, or in any provision of law. In this case, at the time of changes in conditions, any amendment of the rates of interest, commissions, fees and costs in the contract shall be governed by the rules for unilateral amendment of contract set out in these Terms and Conditions and in Business Regulations.
- 12.2./A. If any Reference Rate is terminated or becomes unavailable, based on
- (i) a public announcement made by the administrator of the Benchmark, the regulatory supervisor for such administrator,
 - (ii) a withdrawal of the administrator's rights to provide the Benchmark,
 - (iii) a prohibition under applicable laws or regulations or
 - (iv) a public statement or information by the regulatory supervisor that the Benchmark specifying that it is no longer representative,
- the Bank shall be obliged and entitled to use an Alternative Benchmark defined by the Relevant Nominating Body unless the law of a relevant jurisdiction provides an alternative mandatory rule. The Bank shall inform the Client of the Alternative Benchmark in written form.
- 12.3. The Bank shall debit the fees and costs charged by other – domestic or foreign – banks to the principal/beneficiary and reserves the right for additional debiting or collection of subsequent costs arising in the case of entries managed in the process of domestic or international payments. Foreign bank costs always come in addition to the fees specified in the List of Conditions.
- 12.4. Payment of interests is usually due in arrears, on the last day of the calendar quarter, calendar month, or on the date defined in the contract; due date may also be the expiration date, or the date of termination of the contract. The Business Regulations, the individual contracts or the List of Conditions may provide otherwise.
- 12.5. Payment of fees, commissions and costs is usually due in advance, on the day of concluding the contract, with respect to the entire duration, from the day of entry into force of the contract until the due date/expiration date. The Business Regulations, the individual contracts or the List of Conditions may provide otherwise.
- 12.6. The Bank shall charge the commissions and fees based on the currency of the order in the currency in which the account is kept. Conversion of the fees shall be based on buying/selling rates applicable to the transaction, listed by the Bank.
- 12.7. The Bank can not refund any commission or fee if the order, letter of credit and/or commitment is cancelled or expires in part or as a whole without being used.
- 12.8. On due date, the Client shall provide an amount covering the interests payable as well as any other money claim of the Bank in its bank account/client account (Payment account) maintained with the Bank without any separate notification of the Bank, and the Bank shall be entitled to debit the Client's bank account/client account (Payment account) with the counter-value during monthly closing or on the due date.

Special default interest

- 12.9. In the case of late payment of any cash debt existing on the basis of an agreement between the Bank and the Client – including the case where the balance of the Payment account does not cover the amount of interests, fees and costs debited to the account and payable to the Bank –, the Client shall, for the period extending from the day following the due date specified in the agreement up until the date of settlement, pay the Bank special default interest as defined in the relevant Business Regulations, the List of Conditions or in the individual agreements.

The Client's right to offsetting and the Bank's statutory lien

- 12.10. The Client not falling into the category of the consumer, shall only be entitled to offset its own claims against those of the Bank if the claims of the Client have been recognized by the Bank and/or have been established by a final judgment of the court.
- 12.11. Clients not having any account with the Bank shall pay charges according to the Bank's prevailing List of Conditions. The Bank shall account for charges against the Client's claims towards the Bank.

The Bank's right to offsetting and the Bank's statutory lien

- 12.12. The Bank shall be entitled to debit any of the Client's accounts maintained with the Bank (including any Payment account maintained in foreign currency, and any client account) with its receivables against the Client, arising within the scope of its financial or investment service providing activities.
- 12.13. By signing the Agreement or entering into any other business relationship with the Bank, the Client gives an irrevocable authorization to the Bank to offset any of its claims against the Client against any debts it has towards the Client, including any obligation to pay any amount in the bank account. Furthermore, the Bank shall be entitled to suspend any payment to third parties upon the Client's instructions up to the amount of its own claims, to the extent permitted by law, even if its claims do not arise from the same legal relationship, or they are not yet due but their recovery is deemed uncertain by the Bank. In order to enforce its claims against the Client, the Bank shall be entitled to make any deposit expire and use it before expiration, and in the case of an order for continuous deposit, the Bank shall be entitled to refuse the new deposit order on the due date in accordance with the provisions of clause III.2.18 in order to settle the outstanding debt. The Bank shall not be liable for any damages or costs arising from the suspension of payments as per this section. If currencies of the given account and the debt are not the same, the Bank shall be entitled to use as much funds from the account as necessary to buy the amount required to settle the debt denominated in another currency.
- 12.14. The Bank shall also be entitled to exercise its right to offsetting referred to in section 12.16 in cases where the Bank effected a wrong entry in any of the Client's Payment accounts maintained with the Bank.
- 12.15. The Bank shall be entitled to statutory lien on the Client's payment account claim in security of its claims arising from account management services. Based on

this statutory lien the Bank shall be entitled to deduct its claims arising from account management services from the balance available on the Payment account. The lien shall be considered established when the payment account contract is concluded, without the lien being registered in the collateral register.

13. Jurisdiction and applicable law

- 13.1. With respect to any dispute arising between a domestic legal entity or unincorporated organization as Client and the Bank, the Budapest II or III District Courts shall have exclusive jurisdiction in matters falling within their competences.
- 13.2. With respect to any dispute arising between a foreign legal entity as Client and the Bank, the Permanent Arbitration Court operating as attached to the Hungarian Chamber of Commerce and Industry (Commercial Arbitration Court) shall have exclusive jurisdiction with the application of the Hungarian language in the course of the proceedings, the number of arbitrators shall be three and the parties shall appoint only arbitrator(s) with money and capital market expertise from the arbitration-recommendation list.
- 13.3. With respect to any legal relationship between the Client and the Bank, the laws of Hungary shall apply.

II. TELEPHONE AND ELECTRONIC BANKING SERVICES

1. Common provisions

1.1. Definitions

Within the meaning of this chapter, in addition to section I.2 (Definitions) of the Terms and Conditions:

Service: Telephone (Telefonbank, SMS, Fax) and electronic (Internet Banking, SpectraNet Mobil Banking, Home Banking, UniCredit mBanking mobile application and Private Invest Application) banking services as a whole or any of them.

UniCredit Telefonbank (hereinafter: **Telefonbank**):

The name of the Bank's services available over the phone by dialling +36 1 325 3200 or +36 20/30/70 325 3200 enabling clients to give instructions regarding the account, make inquiries about account balances and other information, as well as ask questions, and report technical problems and Complaints arising while using the Service.

SMS Service: The name of the Bank's service where the Bank, upon request of the Account Owner, sends information related to bank cards or bank accounts/credit card accounts via a mobile telecommunication tool as a text message (SMS).

Internet Banking: The name of the Bank's electronic banking system available through the website of the Bank (www.unicreditbank.hu), enabling clients to give instructions regarding the account, and to make inquiries about account balances and other information. The name 'Internet Banking' includes the services called SpectraNet Internet Banking (Light and Plus) and eBanking.

eBanking: The name of the Bank's electronic banking system to be introduced gradually as described in section 3.2., available for Private Customers through the website of the Bank (www.unicreditbank.hu), enabling clients to give instructions regarding the account, and to make inquiries about account balances and other information.

SpectraNet Mobil Banking: The name of the Bank's electronic banking system optimized on mobile phones, available via suitable mobile phone through the website of the Bank (www.unicreditbank.hu), enabling clients to give instructions regarding the account, and to make inquiries about account balances and other information. The 'Mobil Banking' service corresponds with the service called SpectraNet Mobil Banking (Light and Plus).

Home Banking (Spectra, Spectra Light and MultiCash): the name of an electronic banking system available through a computer (PC), a telephone line and a modem or an internet connection, provided by the Bank based on a separate contract, with the aim of enabling clients to give instructions regarding their Payment accounts, as well as to make inquiries about Payments accounts and other information.

UniCredit mBanking mobile application: The name of the electronic banking service provided through mobile devices suitable for it. The UniCredit mBanking mobile application contains the mBanking and the mToken services which become available after registration (activation). The mToken service used for logging in to the eBanking service and for providing approvals of transactions initiated through eBanking, and the mBanking service allows for the delivery of instructions regarding accounts, as well as making inquiries about account balances and other information.

Private Invest Application: The name of the electronic banking service provided through mobile devices suitable for it that allows, after registration (activation), the use of investment services as determined by the Customer Information of the Private Invest Application, as well as making inquiries about account balances of Payment Account, securities account and other information.

Client Number: an 8-digit code for identifying the Account Owner with the Bank.

User: a person authorized in the Service Agreement or designated on the Bank's appropriate form by the Account Owner to access the telephone or electronic banking system, make inquiries or give instructions regarding the Accounts of the Account Owner; with respect to the exercise of such rights, this term also refers to the Account Owner. Furthermore, User is the Cardholder who possesses Telefonbank User ID and PIN code and has restricted access right for Telefonbank service exclusively related to the bank card held by User.

Biometric identification: an identification method within the frameworks of the UniCredit mBanking mobile application and the Private Invest Application, which enables the Clients to be authenticated by using their fingerprint or in case of Apple mobile devices by using face ID technology (face ID) instead of using a PIN.

VICA application: this application is used to sign in and to submit payment orders to SpectraNet Internet Banking (Light

and Plusz), SpectraNet Mobile Banking, Spectra and Spectra Light systems.

VICA password: The VICA password is created by the User when registering the VICA application, which must be entered by the User each time the VICA application is opened. If the User enables fingerprint authentication in the VICA application, then fingerprint authentication may be used instead of VICA password. If the User has already registered the VICA application - even at another bank - there is no need to create a new VICA Password.

VICA Registration Password: a password provided by the Bank to the User, which is sent by the Bank via SMS to the mobile phone number specified in the User Data Sheet or in the "SCA Setting" order and which is typed in by the User when registering the VICA application at the Bank. Furthermore, User is the Cardholder who possesses Telefonbank User ID and PIN code and has restricted access right for Telefonbank service exclusively related to the bank card held by User.

VICA SMS code: a one-time code provided by the Bank to the User, which is sent by the Bank via SMS to the mobile phone number specified in the User Data Sheet or in the "SCA Setting" order during the registration process of the VICA application. The User completes the registration by typing the SMS code in the selected field of the VICA application. If the registration process is interrupted or the SMS code expires, the registration in the VICA application must be restarted and the Bank sends a new VICA SMS code.

1.2. Use of the Services

- 1.2.1. Except the services of Telefonbank and UniCredit mBanking mobile application available without identification, unless the present General Terms and Conditions and/or the Bank Card Terms and Conditions provides otherwise, the Service may only be used if the Account Owner has concluded a Payment account agreement and/or credit card agreement, or - if the Service allows for the disposition over securities accounts - a consolidated securities account agreement with the Bank, as well as an agreement for the use of the given Service, and has submitted the completed application forms to the Bank as required by the latter. The services of the UniCredit mBanking mobile application and the Private Invest Application services can only be used if the Account Holder has concluded a payment account agreement and/or a credit card agreement, or – if the Service provides for the acceptance of instructions regarding a securities account – a consolidated securities account agreement

with the Bank, as well as the activation of the service in accordance with the relevant rules.

- 1.2.2. The right to use the Service shall adjust to the conditions defined in the individual agreements (in case of service described in section 2.1.1/A conditions are defined in the form) and the conditions set upon the activation of the Service. Standard limits specified in each agreement may be modified following conclusion of the agreement on any bank business day in the Bank's branches in person, as well as through Telefonbank regarding Internet Banking, SpectraNet Mobil Banking or UniCredit mBanking mobile application limits and Telefonbank Transaction Limit. The use of a given Service does not automatically entail the right to access the full range of the Bank's services available, or the telephone and electronic banking services of the Bank to be offered in the future. The starting date of providing the Service shall be at latest the first Bank Business Day following signature of the Service Agreement, or the date fixed in the Service Agreement/on the User data sheet, and for UniCredit mBanking mobile application and Private Invest Application, the day of activation.
- 1.2.3. Upon signing the Service Agreement (and for UniCredit mBanking mobile application and Private Invest Application upon the activation of the service and / or for VICA application upon registration of the application) and thereafter the Account Owner – or the Cardholder who signed the form referred in section 2.1.1/A. - shall continuously ensure, at its own expense, all the equipment and technical background, including hardware and software needed for using the Service, in an operable condition. The Account Owner acknowledges that the Bank shall only undertake to provide the Service if the Account Owner and the User observe the Bank's technical regulations including all amendments thereof, stipulated depending on the given Service and made available to the Account Owner. The Bank shall not be liable for any damages arising from any technical failure of the Account Owner's or User's equipment or from the fact that the User is not able to get into contact with the Bank for this reason.
- 1.2.4. The Service is available on 365 days of the year, 24 hours a day. The Bank reserves the right to interrupt the availability of the Service from time to time for a short period, for example due to system maintenance. The Bank shall send information via the system about the date and time of the expected downtime of the Service.

1.2.5. The Bank is entitled to effect alterations at any time in terms of data transmission, in line with technical developments or in connection with subsequent security measures implemented, and to unilaterally alter, modify, suspend or terminate the system and the Service provided by the Bank.

1.2.6. The Account Owner – excluding the case of restricted access right described in section 2.1.1/A. and if the respective Service provides the possibility – shall indicate in the Service Agreement or on the Bank's form specifically designed for this purpose the name of Users who are authorized to give instructions in connection with the accounts specified in the Agreement/Data sheet through the system of the Service, while identifying such Users in the manner usually required by the Bank. One form grants authorization only within the system related to one specific Service, and is independent of any other methods of giving instructions regarding accounts.

1.2.7. The Account Owner shall report all changes in and withdrawal of the User(s)' authorization using the Bank's form designed for that purpose. The person(s) designated as User on the appropriate form submitted to the Bank shall be considered by the Bank as parties authorized by the Account Owner until receipt of any notification on the change or withdrawal of such authorization. The withdrawal of or change in the user's authorization shall become effective at latest on the Bank Business Day following the effective date of the Account Owner's instruction.

1.2.8. The Account Owner acknowledges that giving instructions through the Services entails risks. The Account Owner or the User is aware that by using the telephone or the Internet, due to the operation of the network there might be cases where the messages sent to each other become known to unauthorized third parties. The Account Owner had taken into consideration this eventuality before choosing the Service.

1.2.9. The Account Owner and the User acknowledge that all transactions, orders as well as their execution carried out by using the Services shall be registered by the Bank's computer system and the transactions effected through telephone operators shall be recorded. In the event of any dispute, the recorded information and data shall be considered as authentic and of full probative value by both

the Bank and the Account Owner/User without the Account Owner/User contesting their authenticity.

1.2.10. The Account Owner acknowledges that the Bank shall only consider an order submitted if it is registered by the Bank.

1.3. Liability, security

1.3.1. The User shall be obliged to keep any password, identifier or identification code (e.g. PIN) depending on the Service (hereinafter jointly: User identifier) confidential, and to ensure that no unauthorized third person(s) may access the User identifier nor the tools (e.g. software, Token, mToken, VICA application, communication key disk, SIM card) needed for using the Service. The Bank shall accept no liability for any damages arising from the non-observance of these obligations or from unauthorized use. The Bank shall be entitled to withdraw the tools necessary for using the Service should their use conflict with the agreement or any provision of law.

1.3.1./A. If the User's mobile device is capable of performing biometric identification (fingerprint or face ID), the User is entitled to identify himself when entering into the UniCredit mBanking mobile application and the Private Invest Application with his fingerprint/face ID and for requests that shall be authenticated in the services of the UniCredit mBanking mobile application and the Private Invest Application (eg transaction approval, debit card limit change) instead of using the PIN code provided that only the biometric data belonging to the Account Holder User has been registered in the mobile device. It is the exclusive responsibility of the User to ensure that the biometric inheritance registered in the mobile device is deleted before the mobile device is removed from the possession of the User for any reason (e.g. device exchange, sale, etc.). The liability for the damage caused by violation of this clause shall be the sole responsibility of the User.

1.3.1./B. Protection of the Credentials in case of Biometric Identification (Fingerprint, Face ID)

- (1) The User shall take all reasonable precautions to protect its credentials and authentication tools from unauthorized access. Otherwise, there is a risk of unauthorized use.
- (2) In order to protect individual credentials

or authentication tools, the User shall pay particular attention to:

- a) Knowledge elements (such as the PIN code) must be kept in secret and it is in particular prohibited to
 - disclose it in verbal communication to a third party (e.g. by phone or in person),
 - enter it in text form into other platform than the Bank's internet banking services (e.g. via email, messenger, etc.),
 - store it in electronic form (for example, store PIN in plain text on the computer or mobile terminal),
 - record it on any device or record and store it with a device that is considered to be a possession element (e.g. TAN generator, mobile device).
- b) in connection with the use the mobile device the User is obliged to
 - make sure that unauthorized persons do not have access to the User's mobile device,
 - make sure that no other person can use the online banking application on the User's mobile device (e.g. mobile phone) (e.g. Online banking application, authentication application),
 - deactivate (render useless) the online banking application (e.g. biometric authentication application) on the mobile device before the device gets out of the User's possession (e.g. the sale or replacement of the mobile phone).

The User's biometric elements (e.g. fingerprints) can only be used as an authentication element on the Internet Banking mobile terminal if the mobile terminal does not store other biometric elements belonging to the User. If the mobile terminal used in the online banking also stores other person's personal credentials, then the User is not entitled to use the biometric authentication, in this case User is allowed to use only the knowledge element (PIN) issued by the Bank.

- 1.3.2. If the Account Owner or the User is aware or may reasonably suppose that the User identifier has become known to any unauthorized third person, or that the tool needed for using the Service get out of his/her possession (including loss or theft of the tool), or that there is an unauthorized transaction in the Payment Account or on

the Account Statement or on any information provided in relation to transactions executed on the securities account, or that any unauthorized payment transaction was initiated against his/her Payment Account using an electronic means of payment, or any unauthorised order was given with respect to the securities held in his/her securities account, the Account Owner or the User shall be obliged to inform the Bank about it immediately in writing, in person, through registered post or over the phone on any day of the year at any time by dialling +36-1 325-3200 or +36 20/30/70 325 3200 (Telefonbank) and to initiate the blocking/ denying of the access or the modification of the User Identifier. The notification shall contain the client number, the user identifier and the description of the event as a minimum. In addition to the above data, the Bank may request further information when the notification is made.

- 1.3.3. Apart from the information specified in the above section 1.3.2, the Account Owner may request the correction of any payment transaction which was not approved or approved but executed incorrectly immediately upon execution of the payment order, but at latest until the day corresponding to the date of debiting of the Account in the second month (in case the Account Owner qualifies as consumer the thirteenth months) following the date of execution of the payment order. If in the month of expiration there is no calendar day corresponding to the date of debiting, the deadline shall expire on the last day of the month.
- 1.3.4. The Account Owner shall be liable for any damages arising prior to the receipt of the written notification or the notification given over the phone in compliance with the prevailing provisions of laws on payment services. For any damage arising after such notifications, the Bank shall be held liable. The Bank shall be released from such liability if it proves that the damage is due to a breach of contract by the Account Owner or the User committed deliberately or through serious negligence (e.g. breach of the obligation to keep security elements safe etc.). The Bank is liable for any incidental damage arising from the use of the Private Invest Application in accordance with the Bank's General Business Conditions on Investment Services and Ancillary Services.
- 1.3.5. The Client is required to use the non-cash payment instrument as stipulated in these Terms and

Conditions, and to display diligent conduct which can be generally expected in the circumstances as regards the safe keeping of the personalized security credentials, the VICA Password, the VICA Registration Password, the VICA SMS code, the Password, and the Security Code necessary to use the non-cash payment instrument (e.g. PIN code, Internet Security Code, mCash code, eBanking one-time log on password). The Account Holder and the User is required to keep the personalized security credentials at a secure place. Should the personalized security credentials get out of the Account Holder's or the User's possession, be lost, stolen or used in an unauthorized or unapproved manner, the Account Holder and the User shall immediately report it to the Bank through Telefonbank or in person in any of the branches. This report shall be made at any time without charging any fees, costs or other payment obligations. When reporting such a case, the identifier of the non-cash payment instrument concerned shall be specified, the Client's name and personal data (date of birth, mother's maiden name) shall be provided. The Account Holder shall be liable for any damages arising from the wilful misconduct or gross negligence of the Account Holder or the User, or from any abuse of the identification data by the Account Holder or the User. In particular, the Account Holder shall solely be liable for any damages arising from the loss, theft or careless handling of the Token, User identifier, mCash code, the VICA Password, the VICA Registration Password, the VICA SMS code, PIN code, Internet Security Code and eBanking one-time log on password or from the access of any unauthorized person(s) to the system and all transactions effected in connection with the account if the Bank proves that the damage was caused by fraudulent actions of the Account Holder or by intentional or grossly negligent breach of its obligations under this Section. The Account Holder shall be obliged to pay damages in such cases if the Bank suffers damages from such events, and if there is evidence that the damage has arisen due to the negligence or wilful misconduct of the Account Holder/User. Violation of security measures set out in these Terms and Conditions shall be considered serious negligence. The Account Holder shall be held liable for the actions of all persons whom he/she enabled to use the Service, either intentionally or through negligence, and such actions shall be deemed as if they had been carried out by the Account Holder. To certify the extent of

damages suffered by the Bank, the Account Holder shall accept the data provided by the Bank, with detailed explanation upon request of the Account Holder.

- 1.3.5/A. The Client shall bear the losses relating to any unapproved payment transactions, up to a maximum of fifteen thousand forints, resulting from the use of a lost or stolen non-cash payment instrument or from the unauthorized use of a non-cash payment instrument occurring prior to the notification. The Client shall not bear the aforementioned liability, if
- a) the theft, or the loss or the unauthorized use of the non-cash payment instrument was not detectable to the Client prior to the payment order,
 - b) the damage was caused by acts or lack of action of an employee, payment service agent or branch of the Bank or of an entity to which its activities were outsourced,
 - c) the Bank does not require strong customer authentication,
 - d) the damage was caused by a personalized procedure that qualifies as non-cash payment instrument, by using an information technology or telecommunication device or if the non-cash payment instrument was used without its personalized security credentials – such as the personal identification code (PIN code) or other code, or
 - e) the Client was not able to make the statement due to the fault of the payment service provider.

If the Account Holder is not a consumer or a micro-enterprise, then the restricted liability provisions of this section shall not apply to the Account Holder.

In the SpectraNet Internet Banking (Light and Plusz), SpectraNet Mobile Banking, Spectra and Spectra Light systems the Bank considers exclusively the VICA application, the SMS authentication and the new type of hardware token device as the strong customer authentication compliant authentication methods. If the Account Holder is not a consumer or micro enterprise, the Bank shall be exempt from Section 45 (2) (c) of the Pft. if the Account Holder or the User has not taken the necessary steps to activate a strong customer authentication method despite the Bank's request (i.e. download and registration of VICA application, updating Spectra program, convert to SMS authentication, receiving and activation of the new type of hardware token device).

1.3.6. The Bank shall accept no liability for any direct and indirect damage arising from the defective operation of the program, not even if the Bank was informed about the possibility of the damage or if the damage was caused by the temporary limitation of the service or the alteration of the program. The Bank may send corrections in case of program errors to the Account Owner on a Durable Medium, through a telephone line or via the Internet. The Bank shall only be liable for damages that have arisen due to the Bank's serious breach of obligations, and only to the extent that the damage was caused by its own serious breach of obligations. In such cases, unrealized profit shall not be considered a damage.

1.3.7. The Account Owner shall be fully liable for all damages caused by computer viruses that have certifiably been transmitted to the Bank through the Account Owner or the User.

1.3.8. The Bank shall define the fee of the Services specified in the prevailing List of Conditions with respect to the present provisions for the restriction or exclusion of liability.

1.3.9. The system of a certain Service may, in justified cases, ban Users or reject the orders submitted in order to make it more difficult to abuse of the system.

1.3.10. Banning or blocking may be avoided if the Service is used properly, which is why the Bank accepts no liability for any damages arising from banning/blocking.

1.3.10/A. The Bank shall bear the risk of sending a non-cash payment instrument or any personalised security credentials relating to the non-cash payment instrument to the Account Holder.

1.3.10/B. When there is a reasonable suspicion of fraudulent use or abuse of a non-cash payment instrument, to safeguard the interests of the Client and minimize the losses of the Bank, the Bank is entitled to temporarily or definitively block or limit the use of the non-cash payment instrument until the circumstances of the event are investigated.

1.3.11. The Bank employs operational monitoring mechanisms to filter out unconventional / suspicious payment transactions, which take into account more risk-based factors when assessing

payment transactions. In the event of a post-transaction check, if it identifies such a suspicious / unusual payment transaction, the Bank may, in some cases, contact the Client on the registered telephone number (from 8:00 to 20:00 on weekdays), even if the Client explicitly excluded the possibility of telephone contact of the Bank. If the Bank does not reach the Client on the telephone number assigned to the contact, the call will also be attempted to other telephone numbers linked to the Client in the Bank's systems (e.g. telephone number specified by the Client for electronic banking services). The Bank shall be entitled to disclose any information about the suspicious / unusual payment transaction and its circumstances only after proper identification of the Client. Shall the identification be unsuccessful, the data related to the bank secrecy with the Client cannot be disclosed, the Bank shall not be liable for any losses incurred due to this and any subsequent steps. If abuse is suspected, the Bank is entitled to temporarily or permanently block or limit the use of electronic banking services to investigate the circumstances of the suspected transaction in order to protect the Client's interests or to reduce its own loss (for example, if the Client does not acknowledge the transaction). The post transaction control does not affect the execution / settlement of the transaction.

1.4. Termination of the Service Agreement

1.4.1. The Account Owner is entitled to cancel the Framework Agreement as well as the Service Agreement at any time without cause in writing, by giving a one-month notice. In this case, the Account Owner shall reimburse all costs incurred by the Bank in connection with termination. The Bank is entitled to cancel the Framework Agreement as well as the Service Agreement at any time without cause in writing, by giving a two-month notice.

1.4.2. If the Account Owner is a client qualifying as consumer or micro-enterprise, any Framework Agreement having been in force for six months or longer may be cancelled by the Account Owner free of any fees, costs and other payment obligations.

1.4.3. If the Account Owner is a consumer, the Account Owner may terminate the Framework Agreement with immediate effect subject to a serious contractual breach of the Bank.

- 1.4.4. If the Account Owner's all Payment account agreements (or consolidated securities account agreements, client account agreements and/or credit card agreements) relevant to a given Service are terminated in any manner whatsoever, the contract relationship related to the use of the given Service shall become invalid upon termination of the last agreement.
- 1.4.5. The Bank shall be entitled to terminate the Service Agreement with immediate effect if:
- a) the Account Owner and/or the User – in case of consumer seriously or repeatedly – violates the Service Agreement or any provisions of the business regulations (including in particular: the secure use and handling of the Service, the handling of the User identifiers, the notification about any change in the clients data recorded by the Bank);
 - b) the Account Owner does not ensure the conditions required for the Service to be used;
 - c) the Account Owner and/or the User does not use the Service properly;
 - d) in case of Business Organization: the Account Owner does not fulfil any of his/her payment obligations arising from the Service Agreement; in case of consumer: the Account Owner delays any of his/her payment obligations arising from the Service Agreement two times consecutively, and fails to remedy such omission within reasonable deadline specified by the Bank in its payment notice;
 - e) the Account Owner and/or the User violates copyright in relation to the software;
 - f) the Account Owner and/or the User attempts to circumvent the security or encryption system of the Service;
 - g) according to the Bank's judgment, any action of the Account Owner and/or the User in connection with any Service is suspected to be a crime, or to be related to a crime.
- 1.4.6. Upon termination the Bank shall be entitled to automatically debit any account of the Account Owner with the costs arising in connection with the installation and use of the software.
- 1.4.7. If the Service is terminated by either party, the Bank shall charge the pro-rata value of the service actually rendered in accordance with the Framework Agreement.
- 1.4.8. For the purposes of the Private Invest Application, the Service is terminated when the Client ceases to hold a Private Banking client status. The Client may terminate the Service by the submission of the User Data Sheet and in accordance with the Customer Information of the Private Invest Application and clauses 1.4.4.-1.4.7 above will also be applicable.
- 1.5. Fees, charges and costs**
- 1.5.1. The Account Owner shall pay a fee to the Bank for the use of the Service. The actual fees of the Services subscribed to by the Account Owner are defined in the agreement to be concluded with the Account Owner and in the List of Conditions. The Account Owner shall pay all fees and costs – including any telephone or Internet access fees – which have arisen in connection with the use of the Service. In case the Bank or another party participating in the transaction, requests a fee, commission or other payment obligation for the use of a non-cash payment instrument, he shall inform the Client thereof prior to issuing the payment order. The Bank does not have any information and does not provide information regarding fees charged by third party providers (TPP). The Client as paying party shall only be obliged to pay fee, commission or perform other payment obligation to the Bank for the use of a non-cash payment instrument if information on the full amount was provided prior to issuing the payment order. The Bank shall be entitled to debit the account designated by the Account Owner or any account of the Account Owner maintained with the Bank with the fees falling due without any further consultation of the Account Owner.
- 1.5.2. The costs shall be debited when they arise or on the last Bank Business Day of every month or quarter as a lump sum. If the Account Owner fails to pay any fee falling due despite being called upon to do so, the Bank shall be entitled to suspend the Service as well as the remote electronic access to the account.
- 1.5.3. The Bank reserves the right to modify the fees as of a specific date by notifying the Account Owner of this fact in advance.
- 1.5.4. The Bank shall notify the Account Holder qualifying as consumer or micro-enterprise of its intention to modify the Framework Agreement at least

2 months – in other cases 15 days – before the proposed modification takes effect. The modification shall be deemed accepted by the Account Holder if he/she does not notify the Bank of the contrary before the modification takes effect. The Account Holder can either accept or reject the amendment of the Framework Agreement before the proposed date of entry into force. In case the Account Holder accepts the amendments, they will entry into force on the proposed date. Rejecting the amendment qualifies as the terminating of the Framework Agreement with immediate effect. The Bank's General Business Conditions on Investment Services and Ancillary Services shall be applicable to any amendment relating to the services provided through the Private Invest Application.

- 1.5.5. Until the date preceding the entry into force of the modification, Account Owners which are clients qualifying as consumer or micro-enterprise are entitled to cancel the Framework Agreement with immediate effect, free of any fees, costs or other payment obligations. In such a case, during the notice period the Account Owner shall pay the Bank the fee that was originally established.
- 1.5.6. If the Client is not a micro-enterprise or a consumer, the Bank is entitled to unilaterally modify the amount of fees according to the Terms and Conditions for Corporate Clients and Municipalities 15 days prior to the effective date of the modification.

2. Telephone banking services

2.1. Telefonbank

2.1.1. Definitions in addition to section I.2 (Definitions) of the Terms and Conditions:

User identifier – a non-secret code composed of digits, used for identifying the User upon entering the Telefonbank system.

PIN code – a 4-digit secret number which is only known to the User; it is used for identifying the User for orders submitted or inquiries made via Telefonbank. The Bank considers this code equivalent to the signature identical to the specimen signature of the Account Owner and of the person with rights of disposition specified by the Account Owner, as provided to and accepted by the Bank. The Bank handles the PIN codes according to strict security requirements, and none of the Bank's employees may know them.

Transaction Limit – the maximum amount of a one-time transfer order relating to a given account of the Account Owner, to be submitted by a given User via the Telefonbank system.

Daily Limit – the maximum amount of transfer orders that can be initiated in total on a given calendar day relating to a given account of the Account Owner, by a given User via the Telefonbank system. The Daily Limit is valid from 0-24 on a given day.

DTMF – Dual Tone Multi Frequency, i.e. TONE operating mode in touch tone telephones.

Operator System – the name of Telefonbank service provided by the Bank's employees.

Automatic System – the name of Telefonbank service available through the Bank's computer system.

Restricted access right to Telefonbank service provided for Cardholders:

- 2.1.1./A. The Bank provides restricted access right to the Telefonbank system for Cardholders with User ID in order to ensure identification process regarding activities exclusively related to bank card held by the User, and in order to execute orders listed in the Form of restricted access right for Telefonbank service. This level of access right does not provide disposal right over the accounts of the Account owner to the Cardholder, the list of available services is defined in the form of restricted access right specifications. The consent of the Account owner is not required to apply for Telefonbank service and use it with restricted access right.

The form of restricted access right specification contains the detailed description of restricted access rights. In addition, provisions of the following sections of the Telefonbank service are also applicable to the Cardholder/User: 2.1.6; 2.1.7; 2.1.8; 2.1.9; 2.1.10; 2.1.11; 2.1.12.

Telefonbank service:

- 2.1.2. The Account Owner may provide access to each of his/her accounts through the Telefonbank system for more than one User at the same time with different authorization levels, depending on the choice of the Account Owner to provide the given User with query rights or rights of disposal over the Account as well. In the case of granting rights of disposal, the Account Owner may assign different

Transaction and Daily Limits to its various accounts for various Users.

- 2.1.3. The provisions regarding activation of a debit card through the Telefonbank automatic system are contained in the Bank Card Terms and Conditions
- 2.1.4. Subject to an agreement with the Bank, the User may have query rights or right of disposal regarding the accounts of several Account Owners at the same time with the same User identifier and PIN code. The Bank does not investigate if the User meets the requirements set out in other legislative provisions.
- 2.1.5. Only the Account Owner in person shall be entitled to modify the group of bank accounts and securities account accessible through the Telefonbank service as well as the method of accessing them.
- 2.1.6. Upon conclusion of the agreement, the Bank hands over the User identifier(s) and a closed envelope with the PIN code(s) to the Account Owner or to his/her authorized representative. In case of the Account Owner or his/her authorized representative having access to eBanking service, the Bank may make available the User identifier(s) and the PIN code(s) to the Account Owner or to his/her authorized representative via eBanking application. The Account Owner shall send the PIN code(s) delivered to him/her in a closed envelope to the given User with the envelope remaining intact. In the case of distribution through commission trade, User identifiers shall not be provided by the Bank upon conclusion of the agreement but subsequently by registered post with return receipt requested to the Account Owner (card holder). The User shall verify the intact condition of the envelope containing the secret PIN code and inform the Bank immediately if he/she finds it damaged. The Bank shall accept no liability for damages arising from the User's failure to provide such notification.
- 2.1.7. Services of the Telefonbank system are available through a touch tone telephone set operating in DTMF mode.
- 2.1.8. In the Telefonbank system, the User may identify himself/herself by entering his/her User identifier and current PIN code using the buttons of the telephone set.
- 2.1.9. In the case of orders given by the User, the system shall verify the right of disposition by checking the PIN code. If a correct PIN code is entered, the Bank shall accept no liability for any damages arising from unauthorized instructions regarding the account.
- 2.1.10. If an incorrect PIN code is entered three times in a row, the User identifier shall be blocked; the User's call shall be received by the operator but in that case the User shall not be authorized to give instructions or make inquiries regarding the account. The operator may release blocking of the User identifier after requesting personal data. After the blocking of the User identifier is released, the old PIN code shall remain valid, and the User may try again to identify himself/herself in the Automatic System. The bank operator shall be entitled to refuse to release blocking of the User Identifier without giving any reason, and in such a case release of blocking of the User Identifier may only be requested in writing in person, in a bank branch. Blocking can be avoided if the PIN code is used properly, which is why the Bank accepts no liability for any damages arising from blocking.
- 2.1.11. The User is entitled to change the PIN code by using the valid User Identifier via Telefonbank's Automatic System as often as required. In case of the User having access to eBanking service, the User is also entitled to change the PIN code via eBanking application as often as required. The Bank shall automatically register the change.
- 2.1.12. The list of services provided through the Telefonbank system is contained in the prevailing client information package pertaining to Telefonbank services.
- 2.1.13. The Account Owner or the User may define the Transaction Limit in the Agreement at the time of signing, or using a form specifically designed for this purpose. The Transaction Limit shall only apply to the transfer orders and transfers between accounts in HUF and in foreign currency effected through Telefonbank services. The maximum amount of Transaction Limits and the default Transaction Limits set by the Bank are contained in the following table. (If the Account Owner or the User does not define any Transaction Limit in the Agreement or on the form specifically designed for this purpose, then the given User, if having a right of disposal, shall be entitled to dispose of the given account up to the default amount set by the Bank.)

Currency of the account	Maximum Transaction Limit to be defined	Default value	
		In the automatic system	In the operator system
HUF	10,000,000	150,000	100,000
EUR	40,000	–	400
USD	50,000	–	500
AUD	70,000	–	700
CAD	60,000	–	600
CHF	60,000	–	600
CZK	1,300,000	–	13,000
DKK	300,000	–	3,000
GBP	30,000	–	300
JPY	5,500,000	–	55,000
NOK	300,000	–	3,000
SEK	350,000	–	3,500
HRK	300,000	–	3,000
PLN	170,000	–	1,700
HKD	350,000	–	3,500
RON	167,000	–	1,670
RUB	1,400,000	–	14,000
TRY	80,000	–	800
CNY*	300,000	–	3,000

* the Bank shall satisfy the orders only in the corporate or SME client groups.

2.1.14. The Account Owner or the User may define the Daily Limit in the Agreement or using a form specifically designed for this purpose. The Daily Limit shall be defined in the same currency as the account currency. In the case of transfer orders denominated in a currency different from the account currency, the limit shall be verified based on the foreign currency mid-rate of the Bank valid on the day of submitting the transfer order. The Daily Limit shall only apply to the transfer orders and transfers between accounts in HUF and in foreign currency effected through Telefonbank services. The maximum amount of Daily Limits and the default Daily Limits set by the Bank are contained in the following table. (If the Account Owner or the User does not define any Daily Limit in the Agreement or on the form specifically designed for this purpose, then the given User, if having a right of disposal, shall be entitled to dispose of the given account up to the default amount set by the Bank.)

Currency of the account	Maximum Daily Limit to be defined	Default value	
		In the automatic system	In the operator system
HUF	9,999,999,999	150,000	3,000,000

Currency of the account	Maximum Daily Limit to be defined	Default value	
		In the automatic system	In the operator system
EUR	40,000,000	–	12,000
USD	51,000,000	–	15,000
AUD	70,000,000	–	21,000
CAD	60,000,000	–	20,000
CHF	60,000,000	–	20,000
CZK	1,300,000,000	–	400,000
DKK	300,000,000	–	90,000
GBP	30,000,000	–	8,000
JPY	5,500,000,000	–	1,600,000
NOK	330,000,000	–	100,000
SEK	400,000,000	–	100,000
HRK	300,000,000	–	90,000
PLN	170,000,000	–	50,000
HKD	350,000,000	–	100,000
RON	167,000,000	–	50,000
RUB	1,400,000,000	–	450,000
TRY	80,000,000	–	25,000
CNY*	300,000,000	–	100,000

* the Bank shall satisfy the orders only in the corporate or SME client groups.

2.1.15. Irrespective of the maximum Daily Limit that can be defined in the Agreement or on the form specifically designed for this purpose, the maximum amount of transfer orders that can be initiated in total on a given day relating to a given account of the Account Owner, by a given User through the Telefonbank's Automatic system is HUF 10,000,000.

2.1.16. The Account Owner acknowledges that if the Bank changes the maximum amount of the Transaction/Daily Limit – in the manner specified in section II.1.5 of these Terms and Conditions – and one or all of the above-mentioned limits defined by the Account Owner exceed(s) that limit, the chosen limit amount shall be changed even without amendment of the individual Agreement to the bank's standard limit, as of the effective date of modification.

2.1.17. The Bank shall execute the User's transaction orders only within the limit over which the User has a right of disposal. The Bank shall execute payments only up to the amount of limit specified in sections 2.1.13 and 2.1.14, and refuse the execution of those exceeding such amounts. The Transaction Limit may be changed by the Account Owner through Telefonbank following identification

in the automatic system, or upon a new written statement of the Account Owner considered as an authorization amending the original form, and submitted accordingly by the Account Owner. The Daily Limit may only be changed upon a new written statement of the Account Owner considered as an authorization amending the original form, and submitted accordingly by the Account Owner.

2.1.18. In the Operator system, the User may provide the particulars of beneficiaries (name, Payment account number) along with a comment for the transfer, in whose favour the User frequently launches transfer order through the Telefonbank system. In such cases only the name of the beneficiary and the amount to be transferred shall be given to the operator.

2.1.19. A prerequisite for launching a transfer order through the Automatic System is that the Account Owner completes, signs and submits the Bank the application form "Transfer Orders specified in advance for using the Telefonbank's Automatic System". On this basis, the Bank shall define the transfer orders so that later the User authorized by the Account Owner can effect transactions by giving the appropriate reference number, the amount to be debited and the additional comment if needed.

2.1.20. Natural persons and sole traders being Users for whom the BA/CA Telefonbank and the "A" service package of the Telefonbank has been activated (based on their current account agreement concluded with the Bank before 30 October 2002):

- can give instructions regarding their accounts according to the provisions of these business regulations through Telefonbank;
- can identify themselves through their previously used identification (Client number) and PIN code in the Telefonbank system;
- are obliged to complete and sign the form specifically designed by the Bank for the purpose of concluding the agreement for the use of the Telefonbank service and specifying access rights, if
 - they wish to use the services of the Telefonbank only for the purpose of account information inquiry in the future, or
 - they wish to specify an amount different from the default Transaction or Daily Limits of the Telefonbank system, or
 - they wish to provide access to their accounts to further Users through the Telefonbank system.

2.2. Fax

2.2.1. The Bank shall conclude no separate agreement relating to the Fax Service, and the provisions of this chapter 2.2. shall apply to Clients who already have such separate agreement.

Accepting payment orders

2.2.2. If the account agreement or the special agreement connected to it expressly provides for it, the Account Owner shall be entitled to send any kind of orders to the Bank by fax, except for orders which must be sent to the Bank in original according to any provision of law.

2.2.3. The option to send messages by fax shall be terminated as of the termination date of the framework agreement.

Rejecting payment orders

2.2.4. The code word specified in the special agreement may only be used for account information inquiry, and does not allow for the submission of orders over the phone. In the absence of code word, the Bank shall accept no orders from the Account Owner by fax.

Data required for payment orders to be executed

2.2.5. The Account Owner is entitled but not obliged to submit the original copy of the order to the Bank. If the original order is submitted to the Bank, it should contain an appropriate and remarkable comment referring to the order submitted earlier via fax (e.g. "previously sent by FAX" or equivalent comment). The Account Owner shall be held liable for any damage arising from the lack of such remarkable comment, including in particular the double execution of orders.

2.2.6. The Account Owner shall not be entitled to send fax messages in order to submit any payment order which, according to the framework agreement or the law, may only be executed against submission of certain documents by the Account Owner or any third party to the Bank, or provided that the Bank or any third party performs a verification of documents or legal titles.

2.2.7. The Account Owner agrees that the Bank handles notifications and orders sent by fax as original ones.

2.2.8. The Bank does not consider orders received by fax as orders submitted on an "original transfer order form". The fees charged for the execution of orders submitted by fax shall be specified in the prevailing List of Conditions.

Arrival and receipt of payment orders

- 2.2.9. The parties agree that the time of arrival of fax messages to the Bank shall be the time recorded on the fax by the fax machine of the Bank's unit managing the order type submitted by the Account Owner.
- 2.2.10. The order of arrival of payment orders received by fax shall be governed by general rules.
- 2.2.11. The Bank shall accept no liability for any damages arising from the falsification of contents and signatures on fax messages or from any other kind of abuses occurred during the sending of fax messages.
- 2.2.12. The Bank shall not be held liable for being unable to perform any order sent by fax due to the insufficient quality of the fax message. If receiving such fax messages, the Bank shall not be obliged to take any action to determine what the payment order relates to. Should any doubt arise about any data of the payment order due to the quality of the fax message, the Bank shall be entitled to refuse to execute the payment order.
- 2.2.13. The Bank shall accept no liability for any damages arising from the inappropriate transmission of data of the fax message or from incorrect or insufficient data, unless they are certifiably imputable to the Bank.
- 2.2.14. The Bank shall only be obliged to restore the content of any fax message if it was damaged or destroyed due to the Bank's fault certifiably, provided that the Account Owner cooperates with the Bank in establishing the data of the fax message.
- 2.2.15. The Bank shall bear no liability whatsoever for damages arising from the fact that the Account Owner's payment order – during transmission of the fax message – is damaged, becomes illegible or is received by unauthorized parties due to the faulty operation or failure of the data transmission connection.

2.3. Text message (SMS) service

- 2.3.1. The Account Owner may request the SMS service, the parameters of the Service and the modification of the Service in writing in the Service Agreement or on the form specifically designed for this purpose, or after identification through the Telefonbank

or Internet Banking or SpectraNet Mobil Banking system.

- 2.3.2. The User may request, modify or delete SMS information service through the Telefonbank or Internet Banking or SpectraNet Mobil Banking system only for the Payment account to which the Account Owner granted him/her access through the Telefonbank or Internet Banking system. Furthermore, the User may request, modify or delete SMS information service only for any bank card with underlying account(s) to which the Account Owner granted him/her access through the Telefonbank or Internet Banking system. If the Account Owner withdraws or modifies the access of the User to the Telefonbank or Internet Banking system, it shall not automatically mean that the SMS service initiated through the system for the given Payment account or bank card will also be terminated. The Account Owner is obliged to provide for the modification or termination of the SMS service separately.
- 2.3.3. Amounts of fees and costs payable by the Account Owner for the SMS service are contained in the Bank's prevailing List of Conditions.
- 2.3.4. The Account Owner shall make sure that the person(s) to whom he/she grants access to the SMS service is/are aware of the conditions related to the service, and the Account Owner shall be held liable for any damages arising from his/her failure to perform this information obligation.

Liability, allocation of losses

- 2.3.5. The Card Holder is aware of the risks inherent in the Service, with special regard to the fact that the Bank shall not be held responsible for any information transferred by SMS and qualifying bank secret comes to the knowledge of any unauthorized third person(s) for any reason(s) which is (are) out of the Bank's sphere of interest.
- 2.3.6. The deadline of sending messages through the SMS service is included in the List of Conditions related to the Service. The Account Owner acknowledges that the Bank shall not be liable for the delayed transfer of SMS messages if this happens due to any reason out of the Bank's sphere of interest.
- 2.3.7. The scope and content of services included in the SMS service are contained in the prevailing List of Conditions related to SMS service as well as in the client information.

3. Electronic Banking services I (Internet Banking and SpectraNet Mobil Banking)

3.1. Definitions in addition to section I.2 (Definitions) of the Terms and Conditions:

User identifier – A series of characters necessary for accessing the Internet Banking and SpectraNet Mobil Banking systems, defined upon concluding the agreement – in the Internet Banking and SpectraNet Mobil Banking Agreement or on the form designed specifically for this purpose –, not yet used by any other User. It shall identify the User and consist of at least 6 and maximum 25 characters (in case of eBanking at least 6 and maximum 21 characters), which may be composed of small and capital letters without accents, and numbers. Punctuation marks (except colons) and spaces are not allowed. For security reasons and to avoid any malicious blocking, it is recommended to choose a User identifier which can not be easily guessed when knowing the User and his/her personal background.

Digital user ID: A unique user identifier necessary for activating the services of the UniCredit mBanking mobile application.

Password, Security Code (hereinafter: Password) – A series of characters necessary for accessing the Internet Banking and SpectraNet Mobil Banking systems and for the authentication of orders. The Password shall be considered by the Bank equivalent to the signature identical to the specimen signature of the Account Owner and of the person with rights of disposition specified by the Account Owner, as provided to and accepted by the Bank.

Hardware Token – if Token is selected as an authentication method, this shall be a tool being the Bank's property and made available to the User, necessary for generating the Password, i.e. a code number depending also on the date of use and the serial number of the tool.

mToken – if mToken is selected as an authentication method, this shall be a software-based and PIN-protected code generator application used for generating Password and for providing approvals of transactions initiated through eBanking and approvals of online card purchases.

PIN code – A 4-digit and 6-16-digit series of characters to be specified by the User and necessary for generating the Password by means of Token or mToken.

Help – A documentation containing detailed information on the operation, use and services of the Internet Banking and SpectraNet Mobil Banking systems as well as other useful information, available in electronic format through the Help

menu of the Internet Banking and the SpectraNet Mobil Banking systems.

Digital Transaction Limit – the new Transaction Limit used for retail clients, after the launch of the eBanking service. The limit is the highest amount of which the User may freely dispose in submitting a given transfer order through eBanking or the mBanking service including transfer orders submitted via payment initiation service providers to the debit of the User's payment accounts which can be reached through eBanking and/or UniCredit mBanking mobile application service. With the launch of the eBanking service, the Digital Transaction Limit that will be set in the eBanking system and the mBanking service is equal to the latest Transaction limit used in the SpectraNet Internet Banking system. If the Client has multiple bank accounts, than the Digital Transaction Limit that will be set is equal to the highest previous limit of his/her accounts, as indicated above. After that, the amount of the Digital Transaction Limit of the bank accounts can only be modified uniformly.

Transaction Limit – The highest amount of which the User may freely dispose in submitting a given transfer order through the SpectraNet Internet Banking or the SpectraNet Mobil Banking systems including transfer orders submitted via payment initiation service providers to the debit of the User's payment accounts which can be reached through SpectraNet Internet Banking and/or SpectraNet Mobil Banking system. The Transaction Limit applies to all transactions resulting in the direct debiting of a given account, except deposit orders, direct debit orders and securities transactions (buying/selling stocks listed at the stock exchange, trading with investment funds, transfer of securities).

Digital Daily Limit – the new Daily Limit used for retail clients after the launch of the eBanking service. The highest amount of which the User may freely dispose on a given day, in relation to a given account of the Account Owner through the eBanking system and the mBanking service jointly including transfer orders submitted via payment initiation service providers to the debit of the User's payment accounts which can be reached through eBanking and/or mBanking service. The Daily Limit applies to all transactions resulting in the direct debiting of a given account, except deposit orders, direct debit orders and securities transactions (buying/selling stocks listed at the stock exchange, trading with investment funds, transfer of securities). After the launch of the eBanking system – and in the UniCredit mBanking mobile application also – the amount used as Digital Daily Limit is the same as the previous Daily limit used in the SpectraNet Internet Banking system.

Daily Limit – The highest amount of which the User may freely dispose on a given day, in relation to a given account of the

Account Owner through the SpectraNet Internet Banking and the SpectraNet Mobil Banking systems including transfer orders submitted via payment initiation service providers to the debit of the User's payment accounts which can be reached through SpectraNet Internet Banking and/or SpectraNet Mobil Banking system. The Daily Limit applies to all transactions resulting in the direct debiting of a given account, except deposit orders, direct debit orders and securities transactions (buying/selling stocks listed at the stock exchange, trading with investment funds, transfer of securities).

3.2. Use and services of the system

The distribution of the Bank's SpectraNet Internet Banking and Mobile Banking services – available in the frame of the Internet Banking service described in section 1.1. – will be ceased in the Private Customer segment according to the scheduling to be announced in separate notice. For Private Customers having an existing SpectraNet Internet Banking and/or SpectraNet Mobil Banking service, the Internet Banking service will be provided through the newly introduced eBanking service according to the time schedule to be announced in the relevant List of Conditions. The Bank will notify the affected customers individually about the details of the eBanking service, the modification of their existing SpectraNet Internet Banking agreement and the termination of the SpectraNet Mobil Banking agreement via the SpectraNet Internet Banking system.

- 3.2.1. The technical conditions of the access to the Internet Banking and SpectraNet Mobil Banking systems are contained in the prevailing SpectraNet Internet Banking, SpectraNet Mobil Banking and eBanking Client Information being an inseparable part of these Terms and Conditions:

For technical backgrounds different from the specifications defined in the Client Information, the Bank shall not guarantee the correct operation of the Internet Banking and the SpectraNet Mobil Banking systems.

- 3.2.2. The list of services available through the Internet Banking and SpectraNet Mobil Banking systems is contained in the prevailing client information related to Internet Banking and SpectraNet Mobil Banking services. The Bank provides the SpectraNet Internet Banking and the SpectraNet Mobil Banking services in the form of two service packages: Internet Banking Light and Internet Banking Plusz, respectively SpectraNet Mobil Banking Light and SpectraNet Mobil Banking Plusz. The eBanking service is provided solely for Private Customers connected to private account packages. If the Customer has a right of disposal via Internet

Banking also regarding corporate or SME client accounts beyond its private bank account, than the Private account can be managed via eBanking, while the corporate or SME account via SpectraNet Internet Banking or SpectraNet Mobil Banking services. In the agreement, the Account Owner shall specify the service package he/she wishes to use (and may even use all of them). Furthermore, the Account Owner shall state on a form specifically designed for this purpose which service package a given User is entitled to use when managing his/her accounts. The User is also entitled to use SpectraNet Internet Banking and SpectraNet Mobil Banking at the same time, but with respect to a given Account Owner only with the same service package (Light or Plusz). Internet Banking Plusz services shall only be set for Account Owners or Users for whom this is specified in the Agreement or on the form specifically designed for this purpose (should the Light or Plusz service package not be named in the agreement or on the form specifically designed for this purpose, the Light package will be set automatically).

- 3.2.3. To access the Internet Banking and SpectraNet Mobil Banking systems, a User identifier and a Password – defined in the related Agreement or on the form specifically designed for this purpose – must be entered. In the case of distribution through commission trade, User identifiers shall not be provided by the Bank upon conclusion of the agreement but subsequently by registered post with return receipt requested to the Account Owner.
- 3.2.4. When using the SpectraNet Internet Banking, eBanking or SpectraNet Mobil Banking, the User or the Account Owner – in accordance with the related Agreement or the instructions given on the form specifically designed for this purpose or given via UniCredit mBanking mobile application – may choose from the following ways of authentication:
 - a) Authentication by hardware Token
 - b) Authentication by SMS
 - c) Authentication by mToken (this way of authentication is not available for SpectraNet Internet Banking and SpectraNet Mobil Banking users)
 - d) Authentication by VICA (this way of authentication is not available for eBanking users)

If the User has both SpectraNet Internet Banking and SpectraNet Mobil Banking access related to a given Account

Owner, the two services can be used only with the same authentication method (by VICA, Token or by SMS). In case the User has access to Spectra/Spectra Light and SpectraNet Internet Banking system as well in relation with the same Account Holder and shall the User initiate in any of the systems the conversion to VICA application or to the new type of hardware token then the Bank automatically converts the User to that kind of authentication method in the other system as well in relation with the given Account Holder.

Form of payment orders

- 3.2.5. If the person authorized to dispose of the account gives a payment order to the Bank electronically (hereinafter: electronic order), the parties agree that the time of receipt by the Bank shall be the time registered by the Bank's computer system. The order of arrival of electronic orders shall be the order of items arrived to the Bank.
- 3.2.6. Electronic orders submitted by the Account Owner which, according to the framework agreement or the law, may only be executed against submission of certain documents by the Account Owner or any third party to the Bank, or only if the Bank or any third party performs a verification of documents, may only be executed after all these obligations are fulfilled.
- 3.2.7. For the scope and amount of electronic orders, the Bank may stipulate limits in the List of Conditions and in these Terms and Conditions. The Bank is entitled to unilaterally modify such limits – even if this is unfavourable to the Account Owner – in the manner specified in these Terms and Conditions.
- 3.2.8. The content and date of the payment order appear on the document containing the payment order in the case of orders submitted on a form, or in the case of other types of payment orders they are contained in the electronic data.
- 3.2.9. **Authentication by hardware Token**
 - 3.2.9.1. The User shall generate the Password to log on to the Internet Banking, the SpectraNet Mobil Banking and the Spectra or Spectra Light systems and to authenticate orders by using a hardware Token.
 - 3.2.9.2. The Bank makes possible the use of different types of physical token devices until the full implementation of strong customer authentication rules. The former distributed hardware token devices shall generate a 6-digit code number
- 3.2.9.3. The Bank shall make the Token available to Users following signing of the Internet Banking, the SpectraNet Mobil Banking or the Spectra or Spectra Light Agreement or the form specifically designed for this purpose by the Account Owner, by handing over the Token to the Account Owner or the authorized person for the period of using the Service. In the case of more than one User, the Account Owner shall arrange for the Token to be handed over to the Users designated on the form. The Bank reserves the right to charge the Account Owner a use fee or compensation fee for the use of the Token provided to him/her the amount of which is specified in the agreement or in the List of Conditions. In the event that the Account Owner does not return all Tokens in a proper condition upon termination of the Service Agreement, the Bank shall be entitled to charge the Account Owner the fee specified in the List of Conditions. Information on the use of the Token can be found in the manual attached to the Token and in the homepage of the Bank.
- 3.2.9.4. The User may change the PIN code of the Token at any time. The User shall be obliged to change the initial PIN code provided when receiving the Token, and later if he/she learns or suspects that the PIN code was obtained by any unauthorized person.
- 3.2.9.5. The User shall use the Token provided by the Bank properly, and maintain it in a good state of preservation. In the event of the Token's failure and upon request of the Account Owner the Bank shall provide for the change of the Token. The Account Owner shall be obliged to return the faulty Token to the Bank. If the Token gets damaged or is lost, the Bank reserves the right to debit the Account Owner's account with the fee of issuance of a new Token specified in the List of Conditions.
- 3.2.9.6. The Bank reserves the right to debit the Account Owner's account with the use fee of the Token handed over free of charge or to terminate the

also depending on the time of use and the serial number of the device, valid for 30 seconds - after the appropriate PIN code is entered into the hardware Token. When using the new type hardware token device, the information appearing on the Internet Banking, the Spectra or Spectra Light interactive interface provides guidance. The new type of physical token devices are the so-called Onespan DP310 hardware tokens starting with serial number 61-1.

Service Agreement if the User does not use the Internet Banking or SpectraNet Mobil Banking system for a long period of time (at least for 3 months) for effecting transactions.

- 3.2.9.7. The program running on the Bank's server checks if the code series generated by the given User through the Token assigned to him/her at a given time, entered by the User when accessing the Internet Banking, SpectraNet Mobil Banking or the Spectra or Spectra Light system or sending orders to the Bank, is the same as the code generated by the Bank's server at the same time, belonging to the Token bearing the given serial number. If there is a difference between the two code series, the server shall refuse access to the system and the sending of the order to the Bank. All transactions that are certifiably initiated by the User logged in with a given User identifier, and authenticated by the Security Code generated by the Token assigned to the User shall in all circumstances be considered by the Bank as transactions initiated by the authorized user of the system. The Bank shall not examine the authority of the person using the User identifier or the Token to use them, nor the circumstances of use.

3.2.10. Authentication by SMS

- 3.2.10.1. The User shall use a normal Password (for multiple uses) to log on to the Internet Banking and the SpectraNet Mobil Banking systems. To log on to the system for the first time, the Bank shall send the User's initial log-on Password in a text message. The User shall be obliged to change the log-on Password immediately after logging on to the system for the first time, and later if he/she learns or suspects that it was obtained by any unauthorized person. The log-on Password may be a series of characters consisting of at least 4 and maximum 12 characters and containing letters without accents and/or numbers, regarding Passwords given or modified after 5 October 2016 a series of characters consisting of at least 8 and maximum 12 characters and containing number, letters without accent (in which at least one small letter and one capital letter is compulsory), which may be freely determined by the User. Regarding Passwords given or modified after 5 October 2016 the system will make distinction between small and capital letters. To make the use of the system even more secure, it is recommended to change the log-on Password at least every 30 days.
In case of every Internet Banking and SpectraNet

Mobil Banking service the Users having SMS authentication will receive a one-time (single) log on password as well at the log on to the system via SMS, which one-time password must be also given to the log on after the Username and the normal Password.

- 3.2.10.2. For the authentication of orders, the User shall use a password sent by the Bank to his/her mobile phone number (specified in the agreement or on the form specifically designed for that purpose) for a single use. In the case of distribution through commission trade, the Account Owner shall use a regular password to log on to the Internet Banking and the SpectraNet Mobil Banking systems, while the authentication of orders requires the use of passwords for a single use sent to the Account Owner's mobile phone number by the Bank in a text message. The Bank shall send the initial log-in password as well as passwords for the authentication of orders in text messages to the User's mobile phone number specified in the Service Agreement.
- 3.2.10.2/A. For Clients using any of the Internet Banking and/or SpectraNet Mobil Banking systems of the Bank with SMS authentication, the transaction approval process for all payment orders initiated on the eBanking interface is amended with a new step: the Client must first re-identify himself / herself with his / her internet bank password for each order confirmation.
After identification, the process proceeds on as usual. The Client receives a one-time code / password in SMS that must be entered in order to complete the eBanking transaction according to the current process. Re-entering the password will allow the Client to be identified more securely.
- 3.2.10.3. The Password sent by the Bank in a text message for the authentication of orders for a single use shall be valid for 5 minutes. If the User performs the authentication of the given order with the password sent in a text message for a single use subsequent to this deadline, the Bank shall refuse authentication.
- 3.2.10.4. The User may change at his/her sole discretion the mobile phone number to which the Bank should send the Password for a single use necessary to authenticate orders.
- 3.2.10.5. The Bank shall only send text messages to mobile phone numbers belonging to networks of domestic GSM service providers.

- 3.2.10.6. The program running on the Bank's server checks if the Password entered by the given User to log on to the system or to send orders to the Bank at a given time is the same as the log-in Password registered on the Bank's server in an encrypted format, or the signature Password sent by the Bank in a text message in order to authenticate the given order. If there is a difference between the two code series, the server rejects access to the system or the authentication of the order. All transactions that are certifiably initiated by the User logged in with a given User identifier, and authenticated by the Password assigned to the User shall in all circumstances be considered by the Bank as transactions initiated by the authorized user of the system. The Bank shall not examine the authority of the person using the User identifier or the Password (mobile phone) to use them, nor the circumstances of use. The Bank shall bear no responsibility for any damage incurred by the Account Owner or any other persons due to any transaction initiated by using the User identifier and authenticated by the Password assigned to it but originating from an unauthorized person.
- 3.2.11. Authentication by mToken
- 3.2.11.1. The User may generate the Password or biometric signature necessary for the authentication of orders submitted via eBanking with the help of mToken as well and approve online card purchases. Authentication by mToken can be chosen from the date set out in the Customer Information. A one-time password generated with the help of the mToken must be also given to the successful log on after the Username and the normal Password.
- 3.2.11.2. In order to use the mToken, Users will need to download the UniCredit mBanking mobile application and activate the mToken function. The mToken function may be activated independently of the mBanking service. The prevailing UniCredit mBanking mobile application Customer Information specifies the client groups with access to the mToken authentication feature.
- 3.2.11.3. Users may request activation:
- a) directly in the UniCredit mBanking mobile application (if the User already has an eBanking User ID and submits orders in the eBanking system with SMS authentication)
 - b) personally in any branch and
- c) by Telephone Banking (after an identification process).
- 3.2.11.4. The process of activation directly in the UniCredit mBanking mobile application: after downloading the UniCredit mBanking Mobile application, the User needs to enter their eBanking User ID and log-in Password in the mToken activation page. Once the User has been successfully identified based on the identifiers provided, the application will display the conditions of using the mToken; if, having read the conditions, the User decides to switch from SMS to mToken authentication for orders being submitted in the eBanking system in the future, User may declare this intention electronically, within the application. Following a declaration of acceptance, the Bank sends the mToken activation code by SMS to the same phone number to which the SMS with the single-use passwords are being sent for the authentication of orders made by the User via eBanking. The Bank then enables the User to activate the mToken (during the validity period of the activation code). After entering the activation code, the User is requested to select a secret code (mToken PIN code) of at least 6 and no more than 16 digits; the User will need to enter this code in the application every time they use the mToken in the future. The Client can also log in to mToken eSign Transaction Approval, Online Card Purchase Approval, and Push Token Transaction Approval by using biometric identification (fingerprint or face ID) instead of using the PIN code. If this feature is available on the device, the Client can activate it in the mToken Settings menu.
- 3.2.11.5. The process of activation in branch: after downloading the UniCredit mBanking mobile application, the activation of the mToken may be requested at any one of our branches, in accordance with the rules on changing the method of authentication. This process involves confirming the Digital user ID associated with the User as well as the phone number to which the Bank is to send the SMS containing the activation code needed for activating the mToken. In the application's mToken activation page, the User needs to provide (enter in the application) the activation ID and the activation code received by SMS. Once the User has been successfully identified based on the identifiers provided, the application will display the conditions for using the mToken; if, having read the conditions, the User decides to switch to mToken authentication for orders being submitted in the eBanking system in the future, they may declare this intention electronically, within the application.

Following a declaration of acceptance, the User is requested to select a secret code (the mToken PIN code) of at least 6 and no more than 16 digits; the User will need to enter this code in the application every time they use the mToken in the future.

The Client can also log in to mToken by using biometric identification (fingerprint or face ID) instead of using the PIN code. If this feature is available on the device, the Client can activate it in the mToken Settings menu.

3.2.11.6. The process of activation by Telephone Banking: after downloading the UniCredit mBanking mobile application, the activation of the mToken may be requested by contacting Telephone Banking, in accordance with the rules on changing the method of authentication. This process involves confirming the Digital user ID associated with the User as well as the phone number to which the Bank is to send the SMS containing the activation code needed for activating the mToken. In the application's mToken activation page, the User needs to provide (enter in the application) the Digital user ID and the activation code received by SMS. Once the User has been successfully identified based on the identifiers provided, the application will display the conditions for using the mToken; if, having read the conditions, the User decides to switch to mToken authentication for orders being submitted in the eBanking system in the future, they may declare this intention electronically, within the application. Following a declaration of acceptance, the User is requested to select a secret code (the mToken PIN code) of at least 6 and no more than 16 digits; the User will need to enter this code in the application every time they use the mToken in the future. The Client can also log in to mToken eSign Transaction Approval, Online Card Purchase Approval, and Push Token Transaction Approval by using biometric identification (fingerprint or face ID) instead of using the PIN code. If this feature is available on the device, the Client can activate it in the mToken Settings menu.

3.2.11.7. The mToken is activated for the eBanking User ID entered during the activation process. Only one mToken may be activated per User ID at any one time, and thus activation of the mToken on a given User ID will result in the deactivation of the mToken that may have been formerly activated on it.

3.2.11.8. Users may change their mToken PIN codes at any time and must do so if they find out (or suspect) that unauthorized persons may have accessed the code.

3.2.11.9. Once an mToken has been activated, the Bank will accept the 6-digit code generated by the mToken for the log-in process for eBanking system and the authentication of orders submitted via eBanking or the biometric authentication enabled by the client. M-Token also manages the approval of transactions received in push message and authenticates the transactions for online card purchases.

3.2.11.10. Depending on which version of the mToken application is downloaded to the device of the Client, Clients using eBanking system can

- a) after selecting the mToken function in the UniCredit mBanking mobile application, the User enters the mToken PIN code or authenticates with a biometric factor; then the mToken generates a 6-digit code, which is valid for at least three, but no more than 3 and a half minutes. The User uses this code to authorize (sign) the submitted orders.
- b) after selecting the mToken function in the UniCredit mBanking mobile application, the User enters the mToken PIN code or authenticates with a biometric factor; then the appropriate option needs to be selected depending on if the generated code is going to be used for log-in process or authorization or approves a transaction in a push message (sign) of transaction. then the mToken generates a 6-digit code, which is valid for at least three, but no more than 3 and a half minutes. Logging in to eBanking can only be done with the code generated for logon, or the Client can only authorize (sign) a transaction with the code generated by the eBanking system to initiate an order. The Client can approve the order by filling in the fields displayed in mToken and eBanking, after either by PIN or biometric identification.

A detailed description of the use of mToken is provided in the effective UniCredit mBanking mobile application Customer Information.

3.2.11.11. The software running on the Bank's server checks the code sequence generated at a given point in time by the mToken allocated to the User (and entered by the User eBanking when submitting their order to the Bank) to see if it is the same as the code generated by the Bank's server at the same time. If the two code sequences differ, the server rejects the

order submittal. Whenever a transaction is proven to have been initiated by the User logged in with the given User ID (and authenticated with a code generated by the mToken allocated to that User), the Bank will consider the transaction as one initiated by an authorized user of the system. The Bank does not investigate whether the person using the User ID and the mToken is in fact entitled to do so, nor does it examine the circumstances of use.

- 3.2.11.12. Further information regarding the use of mTokens is available in the eBanking Customer Information and the UniCredit mBanking mobile application Customer Information.

3.2.11.12/A. VICA authentication

In the SpectraNet Internet Banking (Light and Plusz), the SpectraNet Mobil Banking, the Spectra and the Spectra Light systems the authentication of the User and the payment orders may be executed with VICA application. The downloading and the registration of the VICA application is executed by the User.

In order to use the VICA application and to switch from the previously used authentication mode to the VICA application, the statement of the Account Holder in the User Data Sheet is required or the User himself or herself may initiate the change of the authentication mode using the order available in the "SCA Setting" menu of Spectra/SpectraNet/SpectraNet Mobil systems. Signing a "SCA Setting" order is only possible with a letter signing right. If the authentication mode change is initiated by the User with the letter signing privilege, then the "SCA Setting" order will be signed in the current authentication mode. Upon successful Bank acceptance of the "SCA Setting" order or after the Bank has recorded the statement on the User Data Sheet, the User's authentication method will change to VICA authentication and the Bank will send the VICA Registration Password to the mobile phone number specified in the User Data Sheet or "SCA Setting" order.

In order to use the VICA application, the User needs to register the VICA application using the User ID, the VICA Registration Password and the VICA SMS code. To log into the application the VICA password is required, or if the User permits fingerprint authentication in the VICA application, then fingerprint authentication may be used instead of the VICA password.

After the VICA application is successfully registered, the authorization of orders and Spectra/SpectraNet/SpectraNet Mobil system logins take place in the VICA application. One User may have only one registered VICA application at a time, as a result of which, a new registration process related to that User's User ID will result in the deactivation of the previously registered VICA application.

In the case of VICA authentication, the User is required to provide his / her User ID upon login, after which the User will receive a notification in the registered VICA application, which the User can approve or reject by entering his / her VICA password.

In case of VICA authentication, the approval of orders requires approval after logging into the VICA application.

If the User switches from another authentication mode to VICA authentication, the change in the authentication mode will not affect the value of the User's Transaction and Daily Limit, and they will continue to apply with unchanged amount.

- 3.2.12. The User may at any time switch from authentication by a Token to authentication based on Passwords sent in text messages (and vice versa), based on the written statement of the Account Owner in the form required by the Bank or through Telefonbank following identification, against payment of the fee defined in the prevailing List of Conditions. The User is allowed to switch from SMS authentication to mToken authentication independently according to the activation method described in Section 3.2.11.4. If the User switches to authentication based on Passwords sent in text messages or to mToken authentication, he/she shall return the Token previously made available to him/her to the Bank. In the event that the Account Owner does not return the Token in a proper condition or at all, the Bank shall be entitled to charge the Account Owner the Token compensation fee specified in the prevailing List of Conditions.

- 3.2.13. The Account Owner shall designate in the Agreement or on the form specifically designed for that purpose his/her bank accounts and the levels of authorization at which he /she wishes to provide access rights to a given User to such accounts within the Internet Banking eBanking, and the SpectraNet Mobil Banking services. Should the Account Owner as User have

access to its accounts also through eBanking and mBanking service, the (account)rights, and account assignment can be set only uniformly in the two service. In case of Private Customers having also an existing SpectraNet Internet Banking and mBanking service, the above described unified rights will be set with the introduction of the new eBanking system automatically so, that the wider account assignment / higher account rights will be applied in both services.

In the event that a User also has access to the accounts of a given Account Owner through SpectraNet Internet Banking, SpectraNet Mobil Banking or Spectra or Spectra Light System installed, the authorizations granted to the User for various systems shall be handled in an integrated manner, meaning that the granting of authorization or any amendment thereof in any system Spectra or Spectra Light installed and SpectraNet Internet Banking, SpectraNet Mobil Banking) shall be effective in the other systems, as well. The only exceptions to this rule are Transaction and Daily Limits, in case of Spectra or Spectra Light installed.

- 3.2.14. The Bank ensures the integrated management of orders recorded through the SpectraNet Internet Banking Plusz and SpectraNet Mobil Banking Plusz services and the Spectra or Spectra Light Client Program through an Electronic Mailbox service maintained on a Bank server. The Electronic Mailbox solely serves the purpose of placing orders or removing orders from there through the Spectra or Spectra Light Client Program installed, or the Internet Banking Plusz and SpectraNet Mobil Banking Plusz services so that the order package can be forwarded to a different Spectra or Spectra Light installation location, and these can be accessible through the SpectraNet Internet Banking Plusz and SpectraNet Mobil Banking Plusz services..

Prepared order packages placed in the Electronic Mailbox may be picked up from there by using a different (or the same) Spectra or Spectra Light Client Program installed or the SpectraNet Internet Banking Plusz and SpectraNet Mobil Banking Plusz services in order to perform further transactions (modification, signing, sending to the Bank). An Electronic Mailbox may only be accessed by the Users of Spectra or Spectra Light Client Programs installed as well as those of the SpectraNet Internet Banking Plusz and SpectraNet Mobil Banking Plusz systems who are capable of handling the Client Number assigned to the Electronic Mailbox. In other words, placing the orders

in the Electronic Mailbox shall not mean their sending to the Bank.

- 3.2.15. The service allowing the transmission of orders (from purpose of signing, modification or sending it to the Bank) between the SpectraNet Internet Banking (Plusz and Light) and the SpectraNet Mobil Banking (Plusz and Light) systems is automatically available, neither the use of an Electronic Mailbox detailed in section 3.2.14., nor a separate contract is necessary.

- 3.2.16. Specification of authorizations for the User(s) to dispose of accounts is made by a so-called authorization score in the SpectraNet Internet Banking and SpectraNet Mobil Banking systems.. The authorization score may be specified for each account. In order for the Bank to accept an order, the score of the User signing the order must be at least 10, and if there are several signatories, their total score must be at least 10 (e.g. two signatories should have 5 points each). If the score is zero, then the User, having a log-in Password, shall only have a right of inquiry.

If the Account Owner grants any right of disposal over a given account to the User in the Agreement or on the form specifically designed for this purpose but defines no authorization score, then the given User shall have a default level of authorization set by the Bank over the given account. Default authorization score set by the Bank: 10 points.

If the Account Owner grants any right of disposal over a given account to the User in the Agreement or on the form specifically designed for this purpose, the given User shall exercise these rights in the eBanking and the mBanking service uniformly.

Furthermore, only Users authorized by the Account Holder according to this section are entitled to dispose over the Account Holder's account(s) via a third party service provider (TPP).

In case of eBanking and mBanking service the User may have inquiry and or disposal right, that can be given by the account owner for each account.

- 3.2.17. For sending orders through a free-format letter or any kind of letter as specified in the prevailing client information, it is needed to determine the 'score for signing letters' on the form provided by the Bank. To the score(s) of signature(s) of the User(s) the above provisions shall apply. The prevailing Client Information

shall specify whether the verification of authorizations to sign for a given order type shall be done on the basis of a so-called 'score for signing letters' or based on the authorization score set for the given account.

In the case of business partnerships, the right of corporate signature or the right for signing letters may only be granted to the authorized representatives of the company. The Bank shall not verify the authorizations of the person assigned, so the Account Owner shall be liable for the conformity of the said person to these provisions.

The free-format letter is not available in the eBanking system.

- 3.2.18. In a free-format letter, no orders, instructions regarding any account or any other instructions may be submitted which could otherwise be forwarded directly within the system, using a function available to the given user. The Bank shall execute incoming orders according to its business regulations, and shall disregard any letters whose contents are not in line with or conflict with its business regulations.
- 3.2.19. If the Account Owner granted the User a right of inquiry extending to all accounts – in the Agreement or on the form specifically designed for this purpose –, then the User shall have the right to make inquiries regarding account balances, transactions history and account statements for any current and future accounts of the Account Owner (including bank accounts, client accounts, deposit accounts and credit accounts, as well). The "right of inquiry extending to all accounts" does not include securities accounts. Rights of inquiry or disposal over securities accounts shall be regulated on an individual basis.
- 3.2.20. Balances of deposit accounts as well as the details of individual fixed deposits are accessible for inquiry without any special setting of authorizations to Users who have at least a right of inquiry over the account in which the deposit was made.
- 3.2.21. The User may initiate transfer orders in HUF to the benefit of a payment account maintained with a Hungarian credit institution only by completing a domestic HUF mask (data input field), and transfer orders in a foreign currency only by completing the foreign currency transfer mask. The Bank reserves the right not to execute HUF transfer orders to credit a Payment account maintained with a Hungarian credit

institution if the foreign currency transfer mask was completed, and foreign currency transfer orders if the domestic HUF mask was completed, and such orders may be cancelled by the bank upon notification of the Account Owner on this fact. The Bank shall not be liable for any damages or consequences arising from the non-execution of such orders. In case of eBanking the User may initiate transfer orders in HUF and in foreign currency from the same menu item, where the system automatically decides whether the transaction is HUF or FCY transfer.

- 3.2.22. Transfer orders in HUF to the benefit of a Payment account maintained with a foreign credit institution shall qualify foreign currency transfer orders, so they may only be submitted to the Bank by the User completing the foreign currency transfer mask.
- 3.2.23. The Internet Banking and the SpectraNet Mobil Banking systems enable the use of so-called templates which facilitates the completing of orders submitted in favour of beneficiaries to whom the Account Owner initiates transfers frequently. The Internet Banking and the SpectraNet Mobil Banking systems save the templates by Account Owners; therefore, if a User saves a template, such template may also be managed by another User belonging to the same Account Owner. The templates saved in the Internet Banking system are also available in the SpectraNet Mobil banking system, and vice versa. The eBanking templates are available also in the mBanking service and vice versa.
- 3.2.24. The Account Owner acknowledges that the Bank shall only consider an order submitted if it is successfully sent to the Bank's server. After an order is sent, a confirmation message shall appear on the screen of the Internet Banking or the SpectraNet Mobil Banking system if the order was received by the Bank. If, among the orders sent, there are orders that were not accepted by the Bank (e.g. wrong signature password, or further signatures required), the message appearing shall contain the list of orders rejected together with the reasons of rejection. The Bank shall be entitled to reject any order which, on the basis of these Terms and Conditions or the special business regulations pertaining to different transaction types of credit institutions, cannot be executed. The Bank shall accept no liability for any damages arising from such procedures. The status of orders may be retrieved in the menu item "Sent orders".

3.2.25. The Bank may reject any orders submitted via the Internet Banking or the SpectraNet Mobil Banking system that are sent to the Bank's account management system later than 30 days from signature.

3.3. Security

3.3.1. The User shall be automatically banned (both from the Internet Banking and the SpectraNet Mobil Banking systems) following three unsuccessful attempts in a row to sign in the Internet Banking or the SpectraNet Mobil Banking system with a Password not matching the User identifier, or following three unsuccessful attempts in a row to authenticate an order with a Password not matching the User identifier. Banning of the User can be cancelled based on the written statement of the User provided in the manner required by the Bank or through Telefonbank following identification.

3.3.2. The Token or the mToken shall be automatically blocked following three attempts in a row to generate a Password with a wrong PIN code. Blocking of the Token can be cancelled based on the written statement of the Account Owner or the User provided in the manner required by the Bank or through Telefonbank following identification. The blocking of an mToken may be released by following the rules on activation.

On a suitable mobile device, the User may, at his own risk, permit fingerprint identification of the mobile device or face ID facial recognition on a mobile device, instead of entering the PIN code. The Bank disclaims any liability for any biometric identification errors resulting from the technology. If this feature is available on the device, the customer can activate it in the "Settings" menu of mBanking service. Instead of the PIN code, biometric identification can be used to sign transactions (including instant transfers) made through mBanking service, mCash withdrawals, change debit card limits, activate new and renewed debit cards, sign up for deposit accounts and set up secondary identifiers. If the biometric identification fails, the mBanking service will ask for the PIN code. After three unsuccessful PIN attempts, the User will be automatically banned from the specified service of the UniCredit mBanking mobile application.

3.3.2./A. In case of 3 (three) consecutive unsuccessful attempts to enter the VICA Password for the VICA

application, the User shall be blocked out and only the Bank can allow the unblocking. If the User forgets his / her VICA password, then the VICA application must be reinstalled, for which the Account Holder may request a new VICA SMS code from the Bank.

3.3.3. Banning or blocking may be avoided if the Service is used properly and carefully, which is why the Bank accepts no liability for any damages arising from such actions.

3.3.4. The Bank concludes the Agreement regarding the Service with the Transaction and Daily Limits set by the Account Owner up to the maximum amount of the limits. With the launch of the eBanking system, the new Digital Transaction Limit and the Digital Daily Limit will be set for the affected retail clients' accounts as described in section 3.1.

3.3.5. The maximum amount of the Transaction Limit/ Digital Transaction Limit is HUF 10,000,000 (or its foreign currency equivalent), in case of Users using mToken and/or VICA authentication HUF 20,000,000 (or its foreign currency equivalent); exceptions may only be made on the basis of a separate agreement (the duly defined limit amount is contained in the agreement or on the appropriate authorization form of the User).

3.3.6. Unless the prevailing List of Conditions or announcements related to the given product provide otherwise, the maximum amount of the Daily Limit/ Digital Daily limit is HUF 10,000,000 (or its foreign currency equivalent) in case of Users using mToken and/or VICA authentication HUF 20,000,000 (or its foreign currency equivalent); exceptions may only be made on the basis of a separate agreement. (the duly defined limit amount is contained in the agreement or on the appropriate authorization form of the User) The Daily Limit shall be verified by the system when the order is sent to the Bank; accordingly, the Bank shall reduce the amount of Daily Limit for the User's given Account by the amount of the order on the date of sending. In case the User has both Internet Banking, and SpectraNet Mobil Banking access for a given account, the Daily Limit includes the aggregate amount of the orders sent through any of the above services.

3.3.7. The Bank shall execute the User's transaction orders only within the limit over which the User has a right of disposal. The Bank shall execute payments

only up to the amount of limit specified, and refuse the execution of those exceeding such amounts. Transaction or Daily Limits, Digital Transaction Limit and Digital Daily Limit may only be modified based on the written statement of the Account Owner provided in the manner required by the Bank or through Telefonbank, by the Account Owner, following identification, and in case of the Digital Transaction Limit uniformly for all accounts of the Client.

The Account Owner acknowledges that if the Bank changes the maximum amount of the Transaction/ Daily Limit, Digital Transaction Limit and Digital Daily Limit, and one or all of the limits defined by the Account Owner exceed(s) that limit, the chosen limit amount shall be changed even without amendment of the individual Agreement to the bank's standard limit, as of the effective date of modification.

- 3.3.8. The Account Owner acknowledges that – for the protection of the Account Owners – the Bank is entitled to the unilaterally limitation of the Transaction- and the Daily Limit, Digital Transaction limit, Digital Daily Limit regarding the eBanking and the SpectraNet Mobil Banking with immediate effect without any prior written notification of the Account Owners and the Users – but by notifying them at the same time through the systems – if it is reasonable according to the bank risks, especially in case of mass- or targeted phishing attacks.
- 3.3.9. If the Account Owner or the User does not define any Transaction or Daily Limit in the Agreement or on the form specifically designed for this purpose, then the given User, if having a right of disposal, shall be entitled to dispose of the given account up to the default amount set by the Bank. The default Transaction Limit set by the Bank for bank accounts maintained in HUF is HUF 200,000 and the Daily Limit is HUF 500,000. For bank accounts maintained in euros, the respective limits are EUR 1,000 and EUR 2,000. The default Digital Transaction Limit set by the Bank for bank accounts maintained in HUF is HUF 200,000, the Digital Daily Limit is HUF 500,000, for bank accounts maintained in EUR the limit is equal to 200,000 HUF calculated on the mid-market price of the Bank on the day of submitting the transfer order, the Digital Daily limit is 2,000 EUR.

In the case of Users for whom only one Daily and Transaction Limit had been set in the Agreement or on the form specifically designed for this purpose (i.e. there are no different limits for each bank account), the

limits specified shall apply to each Payment account managed by the User. In this case, limit amounts specified in HUF shall be converted – for FX accounts – using the FX mid-rate of the Bank applicable on 30/11/2007.

4. Electronic Banking Services II (Home Banking)

The Bank's installed Spectra and Spectra Light services – available in the frame of the Home Banking service described in section 1.1. – will be ceased in the Private Customer segment according to the scheduling to be announced in separate notice. For Private Customers (except for Private Banking clientele) having an existing Spectra or Spectra Light Client Program, the Electronic Banking service will be provided through the newly introduced eBanking service according to the time schedule to be announced in the relevant List of Conditions. The Bank will notify the affected customers individually about the details of the eBanking service, and the termination of the Home Banking agreement via the SpectraNet Internet Banking system, and/or in postal mail

4.1. Definitions in addition to section I.2 (Definitions) of the Terms and Conditions:

Client program (CP) – the software made available to the Account Owner by the Bank, which is able to communicate with the given Home Banking electronic bank system ("System").

Initial login password – a code randomly generated by the Bank through the Spectra or Spectra Light System, which ensures the first login to the Spectra or Spectra Light system for the User.

Login password – a code specified by the User following the first login to the Spectra or Spectra Light system, and registered by the System, which can contain both letters and numbers.

Signature password – a code defined by the User and registered by the given Home Banking System, which can contain both letters and figures. The Bank shall consider this password equivalent to the signature identical to the specimen signature of the Account Owner and of the person with rights of disposition specified by the Account Owner, as provided to and accepted by the Bank.

Electronic signature – a series of numbers placed at the end of orders generated by the Home Banking Client program, which constitutes the control amount for the given data, coded by the signature password of the "signatory".

Custom installation program identifier – a code to be used in installing the Spectra or Spectra Light system with the purpose of clearly identifying the system. The identifier identifies the

location, i.e. if the Account Owner wishes to use the same client number at more than one location, it shall require the generation of separate identifiers for each location.

User Manual – an electronic or printed documentation containing detailed information on the operation, use and services of the given Home Banking System as well as other useful information.

Installation Package – includes the Installation Guide, the installation CD-ROM, the Custom installation program identifier and the envelope containing the Initial login password(s).

BPD file, communication key disk – a custom tool to identify the Account Owner or the User (e.g. floppy disk).

4.2. Copyright

- 4.2.1. The Account Owner may use as many copies of the Client program as many authorizations he/she was granted, or as many Client programs he/she paid the one-time entry fee for. One licence of the software shall not be used on more than one computer at the same time.
- 4.2.2. The Account Owner is entitled to make a copy of the software, but the copy shall be used solely for the purpose of safekeeping, protection or archiving.
- 4.2.3. Use of the Client program shall also include the case where the Account Owner stores it in the random access memory (RAM) of a given computer or installs the software on a permanent data storage unit (hard disk, CD-ROM) of a given computer or network server, unless the copy is stored in a network which is only used for forwarding data to other computers.
- 4.2.4. The Bank shall transfer the right of use of the software in accordance with the rules of copyright; therefore, the software shall be regarded as a protected product according to laws on copyright, international treaties and the local regulations in each country. Based on the above, the Client program shall be considered as a product protected by copyright. Copying the User Manual or any written or electronic materials provided with the product is not allowed.
- 4.2.5. The Account Owner is not allowed to transfer the software for use or in possession to third parties, or to grant them a right of disposal over it, but the Account Owner is entitled to transfer its rights deriving from the Service Agreement exclusively to

its legal successor in a definitive manner, provided that the Account Owner transfers all copies of the software and all written materials, and if the recipient enters into an agreement with the Bank.

- 4.2.6. By signing the Service Agreement, the Account Owner shall assume the obligation to preserve the software, the user manual and other information materials provided by the Bank with due care, and to protect them from being used by unauthorized parties, copied, modified or made public.
- 4.2.7. The Account Owner shall be held liable for any damages suffered by the Bank or any third parties due to the breach of the copyright. The Bank shall accept no liability for any damages arising from the unauthorized or improper use of the software. The Account Owner shall be fully liable to pay damages to the Bank in the case of any loss suffered by the Bank due to any damaging of the software, failure to meet any notification obligation, unauthorized use, lending, transfer and/or modification of the software.
- 4.2.8. Should the provision of the service be cancelled by either party, the Account Owner shall be obliged to stop using the system, to delete the software and to return all the tools, data carriers, the User Manual, and any other information materials received from the Bank no later than by the date of termination of the Service Agreement.

4.3. Security

- 4.3.1. The User shall be banned from the system if:
 - a) a wrong login/bank password is entered three times in a row upon login, or
 - b) sending of orders with an incorrect electronic signature of the given User is attempted three times in a row.
- 4.3.2. Following banning, the banned User shall not be able to log on the system even with a correct login password, and the electronic signature generated with his/her correct signature password shall also be refused by the Home Banking System. Banning of the User may be released in the case of Spectra and Spectra Light by the written statement of the Account Owner provided in the form required by the Bank, or in case of MultiCash with the Bank's approval and initialization of a new BPD file. Banning may be avoided if the Service is used properly, which is why the Bank accepts no liability for any damages arising from banning.

4.3.3. Electronic signature(s) and the authorization levels assigned to them are verified by the Bank. Home Banking accepts the electronic signature as being correct if after decoding the control amount of the coded data is matching the content of the set of data submitted with the order signed. Accordingly, the system does not accept electronic signatures if:

- a) a wrong signature password is used when generating the signature, or
 - b) the content of data of the orders is changed following electronic signature.
- If the electronic signature is correct, the Bank declines any liability for any damages arising from the use of the system or any unauthorized disposal over the account.

4.3.4. If an incorrect password is entered, the CP calls the User's attention to this fact and login shall fail. The CP sends a warning message concerning problems with the electronic signature in case of MultiCash at the time of signing, while in the case of Spectra and Spectra Light only when the order package is sent.

4.3.5. The Bank may reject any electronic orders submitted via the CP system that are sent to the Bank's account management system later than 30 days from electronic signature (in case of MultiCash, this only applies to items waiting for remote signature).

4.3.6. The User is obliged to change the initial login password following the first login. By knowing the valid password, the User is entitled to unilaterally modify his/her login and signature passwords at any time.

4.4. Spectra and Spectra Light

4.4.1. By concluding the Service Agreement, the Bank agrees to execute the orders sent by the Account Owner or the User through the Client Program, and to provide information that is available for inquiry through the Client Program. Registration of the CP – which takes place after an order for registration is submitted – may be done as soon as the signature password is set for the authorized User.

4.4.2. The Account Owner shall receive an Installation Guide in a printed form, which contains the most important information needed for the installation of the program. The User Manual containing detailed information on the operation, use and services of the Spectra or Spectra Light system as well as other useful information is available in an electronic format on the

installation CD-ROM, or in the Help menu of the Client Program following installation. The list of services available through the Spectra or Spectra Light system is contained in the prevailing client information related to Spectra or Spectra Light services.

4.4.3.

- a) Specification of authorizations for the User(s) to dispose of accounts is made by a so-called authorization score. The authorization score may be specified for each account. In order for the Bank to accept an order, the score of the User signing the order must be at least 10, and if there are several signatories, their total score must be at least 10 (e.g. two signatories should have 5 points each). If the score is zero, then the User, having a log-in Password, shall only have a right of inquiry.
- b) For sending orders through a free-format letter or any kind of letter as specified in the prevailing client information, it is needed to determine the 'score for signing letters' or score for corporate signature on the form provided by the Bank. To the score(s) of signature(s) of the User(s) the above provisions shall apply. The prevailing Client Information shall specify whether the verification of authorizations to sign for a given order type shall be done on the basis of a so-called 'score for signing letters' or based on the authorization score set for the given account. In the case of business partnerships, the right of corporate signature or the right for signing letters may only be granted to the authorized representatives of the company. If client programs with version numbers below V5.10-01 are used, in the case of orders for deposit making, cancellation of deposit, cash delivery or Investment Funds, the verification of signature authorizations is also performed on the basis of the so-called 'score for signing letters', meaning that in the case of business partnerships such orders may only be submitted by the authorized representatives of the company.
- c) In a free-format letter, no orders, instructions regarding any account or any other instructions may be submitted which could otherwise be forwarded directly within the system, using a function available to the given user. This does not apply to the customs duty (customs and community tax), and to transfer orders concerning the payment of customs deposit, regarding which the customs authority has a right to online inquiry. The Bank shall execute incoming orders according to its business regulations, and shall disregard any letters whose contents are not in line with or conflict with its business regulations.

- d) If the Account Owner granted the User a right of inquiry extending to all accounts – in the Agreement or on the form specifically designed for this purpose –, then the User shall have the right to make inquiries regarding account balances, transactions history and account statements for any current and future accounts of the Account Owner (including bank accounts, client accounts, deposit accounts and credit accounts, as well). The “right of inquiry extending to all accounts” does not include securities accounts. Rights of inquiry or disposal over securities accounts shall be regulated on an individual basis.
 - e) Balances of deposit accounts as well as the details of individual fixed deposits are accessible for inquiry without any special setting of authorizations to Users who have at least a right of inquiry over the account in which the deposit was made.
 - f) If the set of data in a given order does not have the necessary electronic signature(s) worth at least 10 points, the program shall call the User’s attention to this fact upon submission of the order while rejecting the order as well as its execution. The Bank shall accept no liability for any damages arising from such procedures.
- 4.4.4. During the use of the system, the Bank allows for the downloading of account statements to a PC.
- 4.4.5. The system enables the use of so-called templates which facilitates the completing of orders submitted in favour of beneficiaries to whom the Account Owner initiates transfers frequently. The system saves the templates by Account Owners; therefore, if a User saves a template, such template may also be managed by another User belonging to the same Account Owner.
- 4.4.6. The Account Owner acknowledges that the Bank shall only consider an order submitted if it is successfully sent to the Bank’s server. On the screen of the CP, a confirmation message shall appear if the order was received by the Bank’s computer. The Bank shall be entitled to reject any order which, on the basis of these General Terms and Conditions or the special business regulations pertaining to different transaction types of credit institutions, cannot be executed. The status of orders may be retrieved in the menu item ‘Sent orders’.
- 4.4.7. The Bank may reject any orders that are sent to the Bank’s account management system later than 30 days from signature.
- 4.4.8. The Account Owner may initiate transfer orders in HUF to the benefit of a Payment account maintained with a Hungarian credit institution only by completing a domestic HUF mask (data input field), and transfer orders in a foreign currency only by completing the foreign currency transfer mask. The Bank reserves the right not to execute HUF transfer orders to credit a Payment account maintained with a Hungarian credit institution if the foreign currency transfer mask was completed, and foreign currency transfer orders if the domestic HUF mask was completed, and such orders may be cancelled by the bank upon notification of the Account Owner on this fact. The Bank shall not be liable for any damages or consequences arising from the non-execution of such orders.
- 4.4.9. Transfer orders in HUF to the benefit of a Payment account maintained with a foreign credit institution shall qualify foreign currency transfer orders, so they may only be submitted to the Bank by the Account Owner completing the foreign currency transfer mask.
- 4.4.10. The User may carry out the authentication of the User and the payment orders with VICA application or with the new type of hardware token in the Spectra and Spectra Light systems. For the conditions of the registration and usage of the VICA application and also for the conditions of authentication with the new type of hardware token see Sections 1. and 3. of Part II. of the present Terms and Conditions.
- 4.4.11. In case the User has access to Spectra/Spectra Light and SpectraNet Internet Banking system as well in relation with the same Account Holder and shall the User initiate in any of the systems the conversion to VICA application or to the new type of hardware token then the Bank automatically converts the User to that kind of authentication method in the other system as well in relation with the given Account Holder.
- 4.5. Multicash**
- 4.5.1. The Bank delivers the Client program by installing it to the personal computer of the Account Owner together with the User Manual. The description of the Client program and the rules of its use are contained in the User Manual, and the essential technical conditions for the use of the program are included in the Client Information attached

as an Annex to the MultiCash Service Agreement. Upon installing the Client program, the Bank shall provide a one-time training free of charge to the staff of the Account Owner.

- 4.5.2. For a fee agreed upon, the Bank shall deliver the program packages ordered together with the program manual and the communication key disk or signature disk(s), and shall ensure the maintenance of the Client program.
- 4.5.3. The maintenance service of the Bank includes:
- delivering the latest version of the software approved by the Bank,
 - delivering the modifications to the current version of the software,
 - delivering any new documentation,
 - hotline service during working hours (Monday – Friday: 7.30 – 18.10)
- The Account Owner shall pay the fee of all other maintenance services related to the MultiCash service, not included in the above list and provided by the Bank or by a third party on behalf of the Bank. Such fees are payable to the Bank within 8 days from receipt of the invoice.
- 4.5.4. The identification of the Account Owner authorized to avail of MultiCash services is ensured jointly by the communication key disk (BPD file) provided by the Bank, the bank password, and the Electronic signature. The Account Owner may decide at its own discretion and risk to whom and under what conditions it provides access to the MultiCash system.
- 4.5.5. Upon the first login to the system, the Account Owner or the User granted an access right to the MultiCash system by the Account Owner shall change his/her password and define a so-called bank communication password, or, when using an Electronic signature, set the Signature passwords, too. After the initialization(s) the Account Owner shall be able to use the MultiCash Service within the limits of his/her authorization level.
- 4.5.6. The Account Owner shall keep a computer protocol for all order files, archive such protocol and submit it to the Bank upon request. The computer protocol is generated by the program automatically. Turning off this function or deleting the computer protocol is not allowed.
- 4.5.7. If there are any problems or disputes that cannot be resolved by phone or at a meeting in person, objections can be submitted in all cases by

sending a copy of the so-called computer protocols to the Bank.

5. Electronic Banking Services III. (UniCredit mBanking mobile application, Private Invest Application)

5.1. Definitions added to Section I. 2 (Definition) of the Terms and Conditions

UniCredit mBanking mobile application: Shall mean the software downloadable by anyone from the app store belonging to the operating system of the relevant mobile device (application). Without activation, the application grants access to general information on the Bank, ATM and branch office search and the exchange rate information are available as well. For the use of the mBanking service, in addition to downloading the application, activation of the mBanking service is required.

Private Invest Application: Shall mean the software downloadable by anyone from the app store belonging to the operating system of the relevant mobile device (application). For the use of the service, in addition to downloading the application, Activation is also required.

Activation: Shall mean the procedure that enables the User to use the mBanking and mToken services or the Private Invest Application.

User ID: Shall mean a series of characters identifying the User that have not been used by any other user, which is required to use the services of the UniCredit mBanking mobile application or the Private Invest Application service for the first time following the installation of the application on the mobile device.

Digital user ID: A unique user identifier necessary for activating the services of the UniCredit mBanking mobile application and not equivalent of the User ID.

Activation code: A 16-digit series of characters required for the activation into the services of the UniCredit mBanking mobile application or the Private Invest Application service.

Security code, PIN (Personal Identification Number) code: A series of a minimum of 6 and a maximum of 16 numeric characters required for further logins to the services of the UniCredit mBanking mobile application or the Private Invest Application service and for the authentication of the instructions. The PIN code equivalent to the specimen signature of the Account Holder and of the person authorised

to give instructions on the account submitted to the Bank and accepted by the Bank.

Transaction limit: Shall mean the highest amount for which the User can place an order through the mBanking service. The transaction limit applies to all transactions initiated through the mBanking service involving direct debits, except for deposit placement orders and direct debit authorisations.

Digital Transaction Limit: the new Transaction limit used for retail clients, after the launch of the eBanking service. The limit is the highest amount of which the User may freely dispose in submitting a given transfer order through eBanking or the mBanking service. With the launch of the eBanking service, the Digital Transaction limit that will be set in the eBanking system and the mBanking service is the limit which is equal to the latest Transaction limit used in the SpectraNet Internet Banking system. If the Client has multiple bank accounts, than the Digital Transaction Limit that will be set is equal to the highest previous limit of his/her accounts, as indicated above. If the Client does not have a SpectraNet Internet Banking or eBanking service, than the Digital Transaction limit amount is as stated in the mBanking service.

Daily limit: Shall mean the highest amount for which the User can place an order on any given day through the mBanking service. The daily limit applies to all transactions initiated through the mBanking service involving direct debits, except for deposit placement orders and direct debit authorisations.

Digital Daily Limit: the new Daily limit used for retail clients after the launch of the eBanking service. The highest amount of which the User may freely dispose on a given day, in relation to a given account of the Account Owner through the eBanking system and the mBanking service jointly. The Daily Limit applies to all transactions resulting in the direct debiting of a given account, except deposit orders, direct debit orders and securities transactions (buying/selling stocks listed at the stock exchange, trading with investment funds, transfer of securities). After the launch of the eBanking system – and in the mBanking service also - the amount used as Digital Daily Limit is the same as the previous Daily limit used in the SpectraNet Internet Banking system.

Deactivation: shall mean the procedure leading to the termination of the opportunity to use the mBanking service or the Private Invest Application service for every account of the Account Holder kept by the Bank.

mCash function: cash withdrawal transaction initiated by the User with the mBanking service. The User can withdraw the amount stated in the order from the ATMs operated by the Bank

following the successful entry at the ATM of the order and the individual ID code (mCash code) generated for the transaction.

mCash Transaction Limit – the highest amount for which the User can give instructions in one mCash order.

mCash daily limit – the highest amount for which the User can give instructions in one mCash order on a given date.

mCash code: the individual identification code which the User receives with the mBanking service following the successful submission of an mCash transaction order to be used in the cash withdrawal transaction at an ATM operated by the Bank.

5.2. Activation of services

5.2.1. The Bank provides the UniCredit mBanking mobile service to its customers having a payment account contract and/or a credit card agreement, or - if the Service allows for the disposition over securities accounts - a consolidated securities account agreement with the Bank. The Bank provides the Private Invest Application exclusively to its private banking clients. To be able to use UniCredit mBanking mobile application and the Private Invest Application services, the activation of the services is required.

The activation can take place in the following ways:

- a) in case of UniCredit mBanking mobile application and Private Invest Application, in a branch
- b) in case of UniCredit mBanking mobile application, via Telefonbank
- c) in case of UniCredit mBanking mobile application, via UniCredit mBanking mobile application

5.2.2. Activation in a branch

5.2.2.1. The services of the UniCredit mBanking mobile application can be activated in any branch. Activation also requires the Account Holder's personal appearance. The Activation of the Private Invest Application is only possible in a branch where private banking services are available.

5.2.2.2. In the activation, the Account Holder completes and signs the User Data Sheet. In case of the Private Invest Application, only the Account Holder can be the User. Depending on the scope of Service, the User Data Sheet must indicate the products covered by the service and the amounts of the transaction limit and the daily limit. The User Data Sheet contains, furthermore the User ID and the telephone number where the Bank sends

the SMS containing the Activation code required for the activation into the services of the UniCredit mBanking mobile application or the Private Invest Application. In case of the Private Invest Application, the User Data Sheet also indicates the e-mail address to which the Bank sends the e-mail containing the Activation code. With the launch of the eBanking system the new Digital Transaction Limit and the Digital Daily Limit will be set for the affected retail clients.

5.2.2.3. After the receipt of the User Data Sheet, the Bank provides the opportunity for the Account Holder/ User to log into the services systems of the UniCredit mBanking mobile application with the Activation code on the next banking day at the latest.

5.2.3. Activation via Telefonbank

5.2.3.1. The services of the UniCredit mBanking mobile application can also be activated via Telefonbank. Activation is possible in the time frame set out in the UniCredit mBanking mobile application Customer Information that is an integral part of these General Terms and Conditions effective at all times. In this case, activation is conditional upon the proper identification of the Account Holder, - for enterprises the executive officer using Telefonbank –, in the Telefonbank system. In the activation process, the products covered by the service and the amounts of the transaction limit and the daily limit must be specified, as well as the telephone number where the Bank sends the SMS containing the Activation code required for the activation to the services of the UniCredit mBanking mobile application. During the activation a Bank employee discloses the User ID to the Account Holder. The Account Holders can activate the service via Telefonbank only for themselves, and for enterprises for the representative requesting activation via the Telefonbank; activation for further User(s) is not possible.

5.2.3.2. After the conversation regarding to the activation in the Telefonbank system that records all required data, the Bank provides the opportunity for the Account Holder to log in to the services systems of the UniCredit mBanking mobile application with the Activation code on the next banking day at the latest.

5.2.4. Activation via UniCredit mBanking mobile application

5.2.4.1. Customers having eBanking User ID and using SMS authentication for their orders may activate mBanking service directly via the UniCredit mBanking mobile application. Account Holders may activate the service in this manner only for themselves, Activation for further User(s) is not possible. During the Activation the Account Holder is identified based on the eBanking User ID provided by the Account Holder and the log-in Password related to such User ID. Activation is possible from the date and in the time frame set out in the UniCredit mBanking mobile application Customer Information that is an integral part of these General Terms and Conditions effective at all times.

5.2.4.2. Account Holder acknowledges that UniCredit mBanking mobile application is an electronic channel which enables the Bank and the Account Holder to conclude contracts with each other via electronic way. Contracts concluded in this manner are considered as contracts executed in writing. UniCredit mBanking mobile application may be used for the purposes of concluding the contract for using the mBanking service (i.e. the activation of the service) as well as contract(s) for other service(s) as defined in the prevailing UniCredit mBanking mobile application Customer Information inseparably attached to the present General Terms and Conditions.

5.2.4.3. When activating via UniCredit mBanking mobile application, the Account Holder has to provide (enter into the application) his/her eBanking User ID and log-in Password. If the identification of the Account Holder is successful based on the identifiers provided, the application displays the contractual offer of the Bank regarding the mBanking service, which the Account Holder shall review, understand and in case of consent the Account Holder shall make his/her declaration in terms of concluding the contract for the UniCredit Mobile service (i.e. acceptance of the offer of the bank) within the application, in an electronic way. After making the declaration of acceptance, the Bank shall send an SMS containing the Activation code for the activation to the same telephone number where the SMS with the single-use passwords are being sent for the authentication of orders made by the Account Holder via eBanking. Then – during the validity of the Activation code

– the Bank ensures for the Account Holder the first log-in to the mBanking service.

5.2.4.4. The contract for mBanking service enters into force when the Account Holder's declaration of acceptance made in an electronic way becomes available to the Bank. The Account Holder's declaration of acceptance is confirmed immediately by the Bank in form of an in-app message

5.2.4.5. In case of activating the mBanking service via UniCredit mBanking mobile application, the service shall automatically involve all of the accounts held by the Bank based on Payment accounts agreement concluded with the Account Holder, and – if the service allows for the disposition over these accounts, then – all of the accounts held by the Bank based on the credit card agreement, and/or the consolidated securities account agreement concluded with the Account Holder. However, if the Account Holder is already entitled to use the service as a result of a previous activation (e.g. in case of activation on further mobile devices), then neither the scope of accounts accessible via the service, nor the Daily limit/Transaction limit, nor the Digital Transaction limit and/or the Digital Daily Limit defined for the service previously, nor the accidental restriction given as per Section 5.3.9. shall be modified by further activations.

5.2.4.6. Contract(s) concluded via mBanking service as identified electronic way, declaration(s) made by the Account Holder in such way, and the information given by the Bank to the Account Holder in such way shall be placed in the mailbox of the application, and/or shall be sent to the Account Holder as in-app message. Account Holder can access these documents within the application anytime until the deletion by the Account Holder and the Deactivation or other kind of cessation of the service.

5.2.5. The Bank will only send text messages containing Activation codes to mobile phone numbers belonging to the networks of domestic GSM service providers.

5.2.6. The Activation date is the day when the User logs in to the mBanking service system by using the Activation code (in case of multiple Users, the User logging in the earliest).

5.3. The use of the system and its services

5.3.1. The use of the mBanking service and the Private Invest Application services starts on the Activation Date and ends on the Deactivation Date.

5.3.2. The technical conditions for access to the mBanking service and the Private Invest Application services are set out in the UniCredit mBanking mobile application Customer Information and the Private Invest Application Customer Information (hereinafter: Customer Information) that is an integral part of these General Terms and Conditions effective at all times. In the event of using a different technical environment from the one set out in the Customer Information, the Bank provides no guarantee of the faultless operation of the services. The Customer Information effective at all times contains the products/services accessible through the system, as well as the customer groups that can activate the mBanking and the Private Invest Application services.

5.3.3. To log in to the services systems of the UniCredit mBanking mobile application and Private Invest Application services – apart from downloading the respective application – for the first time, the Activation code sent in SMS during the activation process and – except for activation via UniCredit mBanking mobile application – the Used ID or Digital user ID must be typed in. After this, the Users specify their own secret PIN code or enable the biometric identification and for further log ins only this PIN code needs to be typed in or use the biometric identification. If the mobile device is suitable for that, User can allow for his/her own responsibility that in case of log-ins (except for the first log-in), instead of providing PIN code, the authentication of the User shall be performed by the mobile device based on fingerprint identification or on a suitable mobile device with face ID recognition. The Bank excludes its liability for biometric identification errors resulting from the technology. If this feature is available on the device, the client can activate it in Settings menu of the services of the UniCredit mBanking mobile application the Private Invest Application. In case of failure of biometric identification, both applications ask for the PIN code. After three unsuccessful attempts of authentication by PIN code, mBanking service will be automatically disabled. After five unsuccessful attempts of authentication by PIN code, Private Invest Application will be automatically disabled.

On a suitable mobile device, the User may, at his own risk, permit fingerprint identification of the

mobile device or face ID facial recognition on a mobile device, instead of entering the PIN code. The Bank disclaims any liability for any biometric identification errors resulting from the technology. If this feature is available on the device, the customer can activate it in the "Settings" menu of the mBanking service or the Private Invest Application. Instead of the PIN code, biometric identification can be used to sign transactions (including instant credit transfers) made through mBanking service, mCash withdrawals, change debit card limits, activate new and renewed debit cards, sign up for deposit accounts and set up secondary identifiers. In case of the Private Invest Application, biometric identification can be used to sign any order in relation to the services available through such application. If the biometric identification fails, both applications will ask for the PIN code. After three unsuccessful PIN attempts, the User will be automatically banned from the UniCredit Mobile Service. After five unsuccessful PIN attempts, the User will be automatically banned from the Private Invest Application.

- 5.3.4. On a specific mobile device, the mBanking service and the Private Invest Application service can only be activated to a single User.
- 5.3.5. The authentication of payment orders given in the mBanking service takes place by typing in the PIN code.
- 5.3.6. Forms of payment orders in mBanking service
 - 5.3.6.1. Where the person with disposal rights issues a payment order to the Bank electronically (hereinafter: electronic order), the Parties consider the time established by the Bank's IT system as time of receipt by the Bank. For the receipt rank of the electronic orders, the rank within the file as received by the Bank applies.
 - 5.3.6.2. Electronic orders, where under the Framework agreement or legislation the Account Holder or Third party is required to submit a document, or the Bank or a third party is required to examine documents, can only be performed subject to the prior fulfilment of these obligations.
 - 5.3.6.3. The Bank may set limits for the range of electronic orders and their amount in the List of Conditions and in the General Terms and Conditions. The Bank is entitled to amend the limits unilaterally, to the

detriment of the Account Holder, as set out in these General Terms and Conditions.

- 5.3.6.4. The content and the time of the payment order given by the person with disposal right is certified by electronic data.
- 5.3.7. The User will be obliged to change the PIN code provided if they learn or suspects that an unauthorised third party has learned the PIN code. For even more secure use, it is recommended to change the PIN code at least every 30 days.

The program running on the Bank's server will verify if the PIN code/ biometric identifier submitted upon the given User accessing the system at a given time and upon sending orders to the Bank is identical to the PIN code registered on the Bank's server in an encrypted form. If there is a difference between the two code series, the server rejects access to the system and the authentication of the order. The Bank will consider, in all circumstances, the transactions initiated provably by a given User gaining access by a User Identification and authenticated by the PIN code used by the User as if they were initiated by the authorised User of the system. The Bank does not examine the authority of the User of the User Identification and of the PIN code/ biometric identifier for use of the mobile device and/or the User ID and the PIN code or the circumstances of use. The Bank will bear no responsibility for any damage incurred to the Account Holder or any other persons arising from transactions initiated by using the User ID and authenticated by the PIN code/ biometric identifier used in connection with it but originating from an unauthorised person. During the activation process (except for activation via UniCredit mBanking mobile application), the Account Holder can specify if, for a certain product(s), no debit order can be given via the mBanking service or when, for certain product(s), no crediting can take place as a result of transfers between their own accounts.

- 5.3.8. In the course of Activating the mBanking service (except when it is done through the UniCredit mBanking mobil application), the Account Holder may indicate the products in cases of which debit order cannot be given or credit cannot be made as a result of transfers between own accounts through the mBanking service.

- 5.3.9. The Account Holder is required to make a declaration on the dedicated form if they wish to change the products in the mBanking service (including the involvement of a newly opened account), wish to amend the person or authorisation of the Users or the transaction limit or the daily limit or to change the possibility to credit/debit for certain products. The Account Holder is entitled to amend the listed conditions of the service via the Telefonbank – after the proper identification of the Account Holder, and for enterprises the executive officer using the Telefonbank –; however, no new User can be specified via the Telefonbank. The modification of the accounts involved in the mBanking service, and the account rights can happen in accordance with the eBanking rights solely.
- 5.3.10. In the mBanking Mobile service, so-called templates can be set up that facilitate the completion of the orders to beneficiaries who are frequently used by the User for orders.
- 5.3.11. The Account Holder acknowledges that the Bank will consider only those transfers as orders submitted through the mBanking service or the Private Invest Application services which were successfully sent to the Bank's server. After sending the order, a receipt message will appear on the screen of the relevant mobile device if the order was received by the Bank. Where, amongst the orders submitted, there are orders rejected by the Bank (e.g. due to faulty signature password or the necessity of further signatures), a message is displayed with the list of the rejected orders and the reasons for the rejection. The Bank is entitled to reject orders where they cannot be fulfilled under these General Terms and Conditions or the specific business rules on various credit institution transaction types. The Bank will not be liable for any damage caused by such procedures. The status of an order can be queried through on the "Invoices" page, in the account history that loads at the bottom after selecting the specific account .
- 5.3.12. mCash function
- 5.3.12.1. An mCash transaction through mCash function may be initiated by Users who have an active HUF bank account, regardless of whether the Users have an active debit card or not. In order to submit an mCash transaction order, the User shall select in the mBanking service the HUF bank account to which the mCash transaction order relates.
- 5.3.12.2. After the successful submission of an mCash transaction order, the mCash code appears in the mBanking service. The User can use it at any ATM operated by the Bank within the subsequent 5 minutes to withdraw the cash amount stated in the mCash transaction order. After the set period the mCash code shall no longer be valid.
- 5.3.12.3. The mCash code may only be used by the User submitting the mCash transaction order to withdraw cash from an ATM. Should a person other than the User have a try at using the mCash code to withdraw cash, the Bank shall be entitled to restrict the use of the mCash code, and refuse the execution of the cash withdrawal.
- 5.3.12.4. When an mCash transaction is initiated with the mBanking service, the Bank shall not only verify the mCash daily limit and mCash transaction limit, but will also check the balance available in the account (coverage check). The other limits specified for the orders executed with the mBanking service (Daily Limit, Digital Daily limit etc.) do not relate to the mCash transaction. It is a condition of the successful submission of an mCash transaction order and the generation of an mCash code that the amount in the order does not violate the limits indicated above and that the funds required for the execution of the transaction are available in the account. Once the mCash code has been generated, the Bank shall not reserve the transaction amount on the account but runs another coverage check when the cash withdrawal in the ATM initiated with the mCash code is authorised. The Bank shall not be liable if the cash withdrawal intended to be made with the mCash code fails due to lack of funds if the balance of the account has changed between the two coverage checks
- 5.3.12.5. If the systems involved in the authorisation process are out of order in part or in full, no mCash transaction order may be submitted and no cash may be withdrawn with the generated mCash code (the transaction will be rejected).
- 5.3.12.6. If the Bank has any justified claim against the Account Holder or User based on a transaction executed erroneously due to a technical or communication problem, the Bank may exercise

its right of offsetting and debit the bank account selected during the mCash transaction with its receivables.

- 5.3.12.7. The amount involved in the cash withdrawal transaction initiated successfully with the mCash code is reserved on the account selected after the initiation of the mCash transaction when it is authorised by the bank. With a successful cash withdrawal transaction the debit is made on the first banking day after the payment transaction with the same Value Date as the date of debiting. If a cash withdrawal fails, the booking may remain effective for no more than 14 banking days.

5.4. Security

- 5.4.1. The User will be automatically barred from the mBanking service if a user tries to access the services systems of the UniCredit mBanking mobile application with a PIN code not complying with the User Identification three times in a row, or if a user tries to authenticate an order three times in a row with a PIN code not complying with the User Identification. The barring of the User can be lifted based on the written declaration of the User in the form expected by the Bank or through the Telefonbank following identification.

The User will be automatically banned from the services system of the UniCredit mBanking mobile application if two consecutive attempts failed to log in to mBanking service with a biometric identifier corresponding to that User ID, followed by three consecutive PIN attempts failed to log in to mBanking service. The User will also be automatically banned from the services system of the UniCredit mBanking mobile application if two consecutive attempts failed to authenticate the order with a biometric identifier corresponding to a given User ID, followed by three consecutive PIN attempts. The ban may be terminated on the basis of a written statement by the User, as required by the Bank, or via the Telephone Bank, once identified.

- 5.4.2. The User will be automatically barred from the Private Invest Application if a user tries to access the Private Invest Application with a PIN code not complying with the User Identification five times in a row, or if a user tries to authenticate an order five times in a row with a PIN code not complying with the User Identification. The barring of the User

can be lifted in accordance with the Private Invest Application Customer Information.

The User will be automatically banned from the Private Invest Application if five consecutive attempts failed to log in to the Private Invest Application with a biometric identifier corresponding to that User ID, followed by five consecutive PIN attempts failed to log in to the Private Invest Application. The User will also be automatically banned from the Private Invest Application if two consecutive attempts failed to authenticate the order with a biometric identifier corresponding to a given User ID, followed by five consecutive PIN attempts. The ban may be terminated in accordance with the Private Invest Application Customer Information.

- 5.4.3. By using the Service properly, barring can be avoided, therefore the Bank is not responsible for any damage arising from barring/blocking.

- 5.4.4. The Bank uses the Transaction-, Daily-, Digital Transaction- and Digital Daily Limits specified by the Account Holder, which cannot exceed the maximum amount of each limit.

The maximum amount of the Transaction Limit and the Digital Transaction Limit is HUF 10,000,000 (or an equivalent amount of foreign exchange) from which variations may only be possible by individual agreement.

Unless it is otherwise provided in the List of Conditions or the Announcement for the relevant product, the maximum amount of the Daily Limit and Digital Daily Limit is HUF 10,000,000 (or an equivalent amount of foreign exchange) from which variations may only be possible by individual agreement. The system will check the Daily Limit when the order is submitted to the Bank and, based on this, will reduce the amount of the user's Daily Limit on the orders that can be issued via the mBanking service by the amount of the order on the day of its submission.

- 5.4.5. The Account Holder acknowledges that if the Bank changes the maximum amount of the Transaction / Daily Limit and the limit specified by the Account Holder exceeds it, the limit amount shall be changed without amending the individual Agreement to the standard limit of the Bank as of the date of the change becoming effective.

- 5.4.6. If the Account Holder or the User does not specify a Transaction Limit, a Digital Transaction Limit or a Daily Limit or a Digital Transaction Limit on the Bank's dedicated form, or the Account Holder has activated the service via UniCredit mBanking mobile application (regarding section 5.2.4.5. as well), the disposal can take place and instructions can be given up to the default amount in the mBanking service. The default Transaction Limit – Digital Transaction Limit as set out by the Bank is, for HUF payment accounts HUF 200,000, the Daily Limit- Digital Daily Limit is HUF 500,000, and for payment account held in EUR, the limit shall be in EUR equal to HUF 200.000, calculated at a valid mid-rate of the Bank on the day of submitting the transfer order and EUR 2,000, respectively.
- 5.4.7. The Bank executes orders only up to the amount of the limit specified, and refuses the execution of orders above these amounts. The Transaction and the Daily Limit can be modified by the Account Holder based on the written declaration of the Account Holder in the form expected by the Bank or through the Telefonbank following the identification.
- 5.4.8. The User acknowledges that the Bank shall have the right, with regard to the protection of the account holders, to restrict the Transaction and Daily limits with immediate effect in respect of mBanking service unilaterally, even without any prior written notice to the Account Holder or the User, subject to a simultaneous notice sent via the system, if such a measure seems reasonable with regard to the risks of banking operations, including in particular mass or targeted phishing attacks.

5.5. Deactivation

- 5.5.1. If the Account Holder chooses not to maintain the mBanking service for any product, it is required to notify the Bank thereof by completing the dedicated form or via the Telefonbank, after proper identification.
- 5.5.2. Following the submission of the form, or the notification made via Telefonbank, the Bank shall terminate the possibility of using the mBanking service for each account of the Account Holder within one working day (the Deactivation date).
- 5.5.3. Upon Deactivation, the opportunity to use the mBanking service will cease for each User. The Account Holder undertakes to notify the Users associated with it of the Deactivation.
- 5.5.4. In case of Deactivation, or other kind of cessation of the framework agreement related to mBanking service, the Account Holder has to arrange the electroinic dokuments to be downloaded and saved in properly authentic form. In this case Bank shall provide the electronically stored documents free of charge for the Account Holder.
- 5.5.5. After the Deactivation the Account Holder is entitled to re-activate the mBanking service at any time.
- 5.5.6. In relation to the Deactivation of the Private Invest Application, the Private Invest Application Customer Information is applicable.

III. SPECIAL PROVISIONS REGARDING CERTAIN FINANCIAL AND ADDITIONAL FINANCIAL SERVICES

1. Payment Account maintenance

Conclusion of the framework agreement, main rights and liabilities of the parties, preliminary information, persons with rights of disposition, main components of the Framework Agreement

- 1.1. Based on the written payment account agreement and payment service agreement (hereinafter: Payment account agreement) concluded with the Account Owner, the Bank undertakes to open and keep a Payment account (hereinafter: bank account) to handle the Client's financial transactions and pay a certain amount of money to the beneficiary on the Client's order, while the Client undertakes to pay the counter-value of such services. Under the Payment account agreement the Bank shall manage and register the Funds owned by the Account Owner, execute regular payment orders and perform payment transactions against such funds (and in general, in connection with the Payment account), pay interest on the account balance according to an agreement or as per the relevant List of Conditions, and inform the Account Owner of the amounts credited or debited to the Payment account as well as of the balance thereof. The Account Owner agrees to pay the counter-value of services, to make funds available in order to cover the payment orders given against the Payment account prior to their execution, and to pay the amount undertaken by the Bank to be refunded.
- 1.2. Identification of the Payment account used for the execution of payment transactions is based on the Account Owner's full or abbreviated name and individual Payment account number except for instant transfer orders under 1.51./A.
The prerequisite for opening a Payment account is the presentation of documents prescribed by law. Bank accounts opened for registering the money instruments related to the business activity of the Bank's Clients who are domestic legal entities, private individuals subject to value added tax and sole traders shall be handled by the Bank – unless otherwise agreed upon by the parties – as a Cash Account, except the accounts in which the Bank manages the money instruments of the Account Owner over which the latter has no free right of disposal (e.g. custody account, security deposit account, collateral account, or any amounts due to another person upon any other legal title or based on a separate agreement).
- 1.3. The Bank shall accept dispositions on the a Payment account in compliance with the Signature Card from the Client as Account Owner.
- 1.4. The Bank is entitled to change the number of the Client's Payment account by notifying the Client of this fact at least 30 days in advance.
- 1.5. The Bank shall regard the Account Owner as the sole person authorized to dispose of the bank account, unless the Client gives a written authorization to a third person to dispose of the account and notifies the bank of this authorization. The right of disposal and any transfer of such right shall otherwise be subject to the provisions relating to representation. If the Client deceases, the right of disposal of the person having an authorization or a right of disposal over the account shall cease (on the day the fact of death is established). After the Bank obtains knowledge about the Client's death by any means, it shall be entitled to suspend the right of disposal of the authorized person(s) or of the person(s) having a right of disposal over the account at its own discretion until obtaining trustworthy evidence on the fact of death.
- 1.6. The instruction shall contain the precise full and abbreviated name of the Client, the number of the account concerned, and the signature of the person(s) authorized to give the instruction, which must be identical to the specimen signature provided, and, depending on the nature of the instruction, the information prescribed by the Bank or by law, necessary for the order to be executed.
- 1.7. Should the Client provide the authorization or instruction related to the Payment account in a manner that is not customary at the Bank, but is otherwise compliant with its format and content requirements, the Bank may, based on its judgment, perform the instruction.
- 1.8. The Account Owner may grant rights of disposal over the Payment account to third parties in the manner specified in contract provisions for the specific services related to the Payment account as well as in the bank card agreement concluded with the Bank. The Bank shall not examine the relationship between the Account Owner and the authorized person.
- 1.9. The proxy, any amendment thereto and the termination thereof shall be signed by the Account Owner in the same manner as it appears on the Signature Card. The exact content and period of validity of such proxy shall be

determined by the Account Owner. Until any modification or termination of the proxy, the authorized person – within the scope of the proxy – shall be granted the rights and bound by the obligations of the Account Owner's authorized representatives.

- 1.10. In contrast to the provisions of the section "Representation" of these Terms and Conditions, the Account Owner may grant rights of disposal over the payment account to third parties also on an 'ad hoc' basis. Such an 'ad hoc' proxy may be accepted by the Bank, provided that it is put into a public document or a private document providing full evidence. In the event of any suspicion, any inaccuracy in the data of the proxy issuer or the proxy holder or in any other important items of the proxy, or any unclear information or any suspected abuse, the Bank shall be entitled to refuse the execution of payment orders submitted based on such a proxy, and to call upon the proxy issuer to make a new statement.
- 1.11. Rights of disposal of the proxy holder shall not entitle him/her to make any legal statements to assign new proxy holders, or to change or terminate the authorizations of any proxy holders.
- 1.12. The Bank shall not be liable for any delayed or faulty execution if this was due to any wrong, insufficient or inconsistent information in the payment order or notification of the proxy holder, or to any failure to provide notification on changes in his/her data submitted.
- 1.13. The Bank shall examine the presence and authenticity of signatures on payment orders by comparison with the ones provided on the Signature Card. Any legal entity being an Account Owner shall acknowledge that in its relations with the Bank, the company stamp potentially used by it shall solely serve to state the name of the company, and the Bank shall not examine the presence, form or content thereof nor assume any liability for doing so. If the payment order bears a signature different from the one given on the Signature Card, the Bank shall return the payment order unfulfilled to the sender by stating the reason, or may choose to request a confirmation over the phone at its discretion. The Bank shall be entitled to record such phone confirmation, to which the Account Owner gives his/her consent by accepting this Framework Agreement. Any changes of which the Bank is notified shall be taken into account by the Bank from the date of confirmation of such notification.
- 1.14. Cash may be deposited or withdrawn in the branch offices of the Bank at the cash desks. In addition, Clients holding bank cards may also avail of the automatic teller machines (ATM), or use the cash desk of another payment services provider providing such service.
- In case of cash withdrawal, the Bank shall require proof of the identity of the person making withdrawal, and of his/her authorization to withdraw cash. Cashier hours: the Bank reserves the right to deviate from either the opening hours of the branch office or the opening hours of another cash-desks. Furthermore the Bank reserves the right to occasionally deviate from the cash-desk hours published as well, by complying with the provisions of the law. The Client's obligations regarding preliminary notification on intended cash withdrawals as well as value limits are contained in the prevailing List of Conditions. With respect to cash deposits made at the cash desk, the Client shall be liable for the accuracy and veracity of the legal title specified for the payment, and the Bank shall not examine it unless it is bound to do so by law. Should the money the Client intends to deposit be or seem to be forged or counterfeit, the Bank shall take it down on record, withdraw the said money from circulation and send it to the National Bank of Hungary (MNB) for investigation without delay. The receipt of such money – whether prior to the conclusion of the investigation or when the MNB ascertains that the money is forged or counterfeit and withdraws it from circulation – shall not give rise to any financial claim on the part of the Client. The Bank shall notify the Client by phone in the event of a suspected or actual fraud or security threat detected by the Bank. In case the suspected or actual fraud or security threat affects a large number of Clients, the Bank shall publish relevant information on its website or the electronic entrance page of the Bank's services.
- 1.15. The Bank shall perform funds transfer transactions exclusively in forint or in convertible foreign currencies.
- 1.16. The Bank shall pay interests for the claims registered in the Client's Payment account according to the prevailing List of Conditions and shall settle it in the account by the due date set in the List of Conditions without any special instruction of the Client.
- 1.17. The bank calculates the interest paid to the Client on the basis of the number of calendar days, using the following formula:
$$\text{interest} = \frac{\text{principal} \times \text{interest rate (\%)} \times \text{number of calendar days}}{36\,500}$$
- 1.18. The Bank shall charge the fees and commissions specified in the prevailing List of Conditions for managing the Client's accounts and for effecting cash transactions therein. Such fees and commissions shall be debited by the Bank to the

Client's Payment account on the due date specified in the List of Conditions, without any special instruction of the Client.

1.19. Unless otherwise agreed between the Bank and the Client, on each Bank Business Day when there is any debit or credit entry in the Client's Payment account, the Bank shall prepare and send a bank account statement – qualifies also as "egyenlegközlő" as defined in the Civil Code – of such debit and credit entries and balance of the account of such debit and credit entries to the Client on paper or, based on a separate agreement, electronically.

1.20. The Payment account agreement is concluded for an indefinite period of time as a Framework Agreement, and as such it shall contain not only the conditions of opening accounts but also all essential conditions for future payment orders and payment transactions.

1.21. Deleted provision.

1.22. Deleted provision.

1.23. Deleted provision.

1.24. Deleted provision.

1.25. Deleted provision.

1.26. Deleted provision.

Payment transactions, payment orders and methods of payment

1.27. Any payment transaction – except official transfers and summons for transfers – shall only be executed if the paying party approved it in advance (or subsequently, in the cases specified in the Payment account agreement).

1.28. Methods of payment that can be applied in payment transactions are cash payment, payment between Payment accounts, cash payment related to the Payment account, and payment without Payment account; more specifically:

- a) **Methods of payment between Payment accounts:**
 - aa) transfer, including instant payment transfer,
 - ab) collection,
 - ac) payment initiated by the paying party through the beneficiary,
 - ad) documentary credit (letter of credit).
- b) Methods of cash payment related to the Payment account, in particular:
 - ba) issuance and cashing of cheques for payment in cash,

- bb) cash deposit in payment accounts,
- bc) cash disbursement from payment accounts.
- c) Methods of payment without Payment account, in particular:
 - ca) cash transfer.

Detailed rules of the above-listed methods of payment are governed by the MNB's decree No. 35/2017. (XII. 14.) on cash transactions.

Main features of the services related to methods of payment to be applied in payment transactions in the case of methods of payment between Payment accounts:

Transfers, general rules for transfers

1.29. By submitting a payment order for bank transfer (transfer order), the Account Owner as paying party gives an instruction to the Bank to transfer (settle) a given amount against his/her Payment account in favour of the beneficiary's payment account.

1.30. The transfer order shall be submitted by the Account Owner as paying party to the Bank as payment service provider managing the Account Owner's Payment account.

1.31. Based on an agreement with the payment service provider, the transfer order may also be submitted with a debit date.

1.32. If the date specified as debit date does not fall on a working day, or there is no such a date in the given month, then the following working day shall be considered as debit date.

Transfers, specific rules for transfers

Batch transfers

1.33. In case of batch transfer, the Account Owner as paying party – based on an agreement concluded with the Bank as the Account Owner's payment service provider – may submit transfer orders having the same legal title but directed to different beneficiaries in the form of batches, at the place and in the manner set out in the framework agreement. Partial payment cannot be made for a bulk transfer order. The payment service provider managing the account of the beneficiary shall inform the payment service provider managing the payment account of the paying party about any non-performance (failed crediting) of the batch transfer order as well as about the reason thereof. The payment service provider managing the payment account of the paying party shall forward such notifications (failed orders) to the paying party electronically.

Standing order

1.34. By submitting a standing order, the Account Owner as paying party gives an instruction to the Bank to transfer a given amount regularly, on fixed dates (debit dates). The Bank shall execute the standing order as long as such order is not withdrawn by the Account Owner as paying party, or until the last date of performance specified in the order expires.

Official transfers and summons for transfer

1.35. In judicial enforcement procedures, administrative enforcement procedures and tax execution procedures, financial claims shall be settled through the respective action of the party authorized to issue official transfer orders or summons for transfer by means of official transfer or in accordance with the instructions of the summons for transfer.

1.36. In case of official transfer, the payment service provider of the paying party shall debit the payment account of the paying party with a given amount that shall be credited to the payment account specified by the issuer of the official payment order.

1.37. If any Client who is an Account Owner is entitled to issue official transfer orders, he/she may initiate an official transfer through the Bank, which shall be obliged to forward it to the payment service provider of the debtor in the official transfer transaction.

1.38. In the case of official transfers and transfers based on summons, the Account Owner as paying party shall not be entitled to exercise any right to adjustment.

1.39. Receipt of the official transfer order shall not be refused either by the paying party or by the payment service provider of the party entitled to initiate official transfers.

1.40. Financial claims to be settled according to the instructions of official payment orders or summons for transfer shall be governed by these Terms and Conditions as well as by the MNB's decree No. 35/2017. (XII. 14.) on cash transactions.

Domestic transfers in HUF

Bank transfers or transfers between accounts within the Bank

1.41. Main features of the service: In executing transfers in HUF initiated by a client to the benefit of another client, or transfer orders to be performed between the client's own accounts, the Bank shall debit the payment account of the paying party and credit the payment account of the beneficiary. If such a transfer qualifies as an instant transfer within the meaning of Section III.1.51/A of these Terms and

Conditions, the Bank shall execute the given transfer with the exceptions specified therein.

1.42. Data and individual identifiers necessary to execute payment orders: Number of the account to be debited, name of the paying party, amount to be transferred, currency of the transfer (always HUF), Payment account number of the beneficiary (or, if the transfer in question qualifies as an instant transfer: secondary account ID), name of the beneficiary.

GIRO (transfer)

1.43. Main features of the service: The GIRO transfers are performed in the intraday or overnight settlement system of the GIRO, the orders are executed by the Bank as it is set out in the List of Conditions. Transfer orders in HUF initiated by the client shall be forwarded by the Bank through the Interbank Clearing System operated by GIRO Elszámolásforgalmi Zrt to the beneficiary's payment service provider.

1.44. Data and individual identifiers necessary to execute payment orders: Number of the account to be debited, name of the paying party, amount to be transferred, currency of the transfer (always HUF), Payment account number of the beneficiary, name of the beneficiary. The order shall not be qualified as domestic HUF transfer order if the order was submitted as domestic HUF transfer order but the currency of the Payment account to be debited or to be credited is different from HUF and therefore the data other than those specified in this section plus the comments shall not be considered by the Bank.

VIBER

1.45. Main features of the service: Transfer orders in HUF initiated by the client shall be forwarded by the Bank through the VIBER (Valós idejű bruttó elszámolási rendszer; 'Real Time Gross Settlement System') operated by MNB to the beneficiary's payment service provider.

1.46. Data and individual identifiers necessary to execute payment orders: Number of the account to be debited, name of the paying party, amount to be transferred, currency of the transfer (always HUF), Payment account number of the beneficiary, name of the beneficiary.

1.47. The Bank shall credit incoming amounts received through VIBER to the benefit of the Client immediately the amount is credited to the Bank's account, and shall do so with the same value date, in order that the incoming amount may cover the Client's payment orders of that day. Should the incoming amount transferred through VIBER be credited to the Bank's account after the closing time of VIBER

Client items, the Bank shall make the credit entry with the same value date but at the time specified in the prevailing provisions of law and regulations on cash transactions.

- 1.48. Upon the Client's written request, the Bank shall execute the Client's Order through VIBER (Valós idejű bruttó elszámolási rendszer; "Real Time Gross Settlement System", hereinafter: VIBER). The Bank shall only receive payment orders for execution via VIBER that are denominated in forints and directed to a beneficiary which maintains an account with another domestic bank being a VIBER member. In the prevailing List of Conditions, the Bank defines detailed rules relating to the time of acceptance and execution of Orders.

Batch transfer

- 1.49. Main features of the service: Transfer orders in HUF initiated by the client shall be credited by the Bank to the beneficiary's account maintained with the Bank or forwarded by the Bank through the Interbank Clearing System operated by GIRO Elszámolásforgalmi Zrt to the beneficiary's payment service provider. The amount debited shall appear in the account of the paying party as a single amount.
- 1.50. Data and individual identifiers necessary to execute payment orders: Number of the account to be debited, name of the paying party, and for each transfer: the amount to be transferred, currency of the transfer (always HUF), Payment account number of the beneficiary, name of the beneficiary, legal title of the transfer. Partial payment cannot be made for a bulk transfer order.
- 1.51. Batch transfer orders shall only be accepted by the Bank through an electronic banking system.

Instant payment-transfer

- 1.51/A.1. Essential features of the service:

An individual transfer order for a HUF amount is considered an instant transfer order if

- it is debited to the Payer's HUF payment account,
- it does not exceed HUF 10 million,
- it does not include the debit date following the date of receipt by the Bank,
- it is submitted by the Paying Party by means of information technology, telecommunication means in accordance with Section II. and is processed by the Bank in a manner that does not require human intervention, and
- it is not submitted in batches for a non-consumer Payer (individual batch transfer orders submitted by a payer qualifying as a consumer and fulfilling the conditions under points (a) to (d) are considered as instant

payment orders. Batch transfer orders submitted by non-consumer customers are not executed through the instant payment system.

The Bank shall forward the details of the payment order qualifying as instant payment order to the payment service provider of the beneficiary no later than five seconds after receiving the payment order.

The Bank shall immediately refuse to execute a payment transaction forwarded by the payment service provider of the payer, stating the reason for the refusal, if, according to the data transmitted to it, the time period counted from registered receipt date of the transfer order by the payer's payment service provider exceeds 20 seconds.

If the payment transaction between the payer and the payee is executed between payment accounts held by the Bank, the Bank shall immediately reject the execution of the payment transaction if the time period counted from the registered receipt date of the payment order exceeds 20 seconds.

As soon as the payee's payment service provider is informed of the payment transaction, it shall inform the payment service provider holding the payment account of the payer on the refusal, including the reason for the refusal, or on the execution of the payment transaction, within five seconds of being notified of the transaction, to the payment service provider of the payer's payment account. Thereafter, the Bank shall promptly notify the Paying Party of the information on the refusal to execute the payment transaction, stating the reason for the refusal.

If the payer has submitted the instant transfer order with the beneficiary's secondary account ID, the Bank shall refer to this secondary account ID as the payee's information in any subsequent communication provided in accordance with Pft. . The non-executable instant transfer order shall be immediately refused by the payment service provider of the payer and shall be sent or made available to the payer via the electronic channel used by the Customer for the submission of the instant credit transfer order.

The Bank shall not queue an instant transfer order due to lack of coverage.

Partial payment cannot be made for an instant transfer order. In the case of an instant transfer order, the Bank shall ensure that the amount of the payment order submitted by the Payer is credited to the account of the payee's payment service provider within five seconds of receiving the order.

By way of derogation from paragraph 3, in the case of instant transfer, the payment service provider shall effect the debit and credit on the value date on which the payer's payment account is actually debited and the payee's payment account is actually credited.

In the event that the Account Holder is the beneficiary of an instant transfer, the Bank, as the payment service provider of the beneficiary, shall immediately

- value date of the payment transaction on the value date,

- b) make the amount of the payment transaction available to the Account Holder in a manner that the Account Holder can dispose of immediately and in full; and
- c) irrevocably increase the Account Holder's claim on the Bank by the amount of the payment transaction.

1.51/A.2. Data and unique identifiers required for the execution of a payment order: The payment identification number of the account to be debited, the name of the payer, the amount to be transferred, the currency of the transfer (always Hungarian Forint), the payment identification number of the beneficiary account.

Secondary account identifier

1.51/B.1. An instant transfer order may also be submitted with the Secondary Account ID assigned to the payee's payment account instead of the payee name and payment identification number. Unless otherwise provided by the Account Holder, the Account Holder may identify the Account Holder's payment account as a secondary account identifier with a mobile phone number including a country code referring to an EEA State as a geographic area, an electronic mail address, a tax identification number or tax number. By filing with a bank (assigning a secondary account ID). Unless otherwise provided by the Account Holder, Eligible is subject to Section 1.51 / B.2. above, you may at any time request the Bank to modify or delete the assigned secondary account ID.

1.51/B.2. The person entitled to dispose over the account may assign, modify or delete the secondary account identifier contained in Point 1.51/B.1. as set forth in the List of Terms and Conditions, which shall be an integral part of these Terms of Business.

1.51/B.3. The person entitled to dispose over the account may assign multiple secondary account identifiers to a payment account, but may only assign one secondary account identifier only to one single payment account.

1.51/B.4. Either the Account Holder or any other person entitled to dispose over the account makes the assignment pursuant to Point 1.51/B.1 the assignment shall be accompanied by the consent of the natural person entitled to the secondary account identification approving that:

- a) its name, the IBAN of the payment account included in the assignment and the assigned secondary account ID are handed over to the central database operator, which

will process these data until the statement of consent is withdrawn or the regular annual data review by the Bank is unsuccessful; .

- b) (b) its data referred to in point (a) shall be forwarded by the central database operator to financial institutions and other service providers not qualifying as financial institutions engaged in processing, settlement and fulfilling payment orders for the purposes of providing payment services and processing and settlement of payment orders and for the transmission of payment requests.

1.51/B.5. In case other person than the natural person account holder is entitled to give its consent pursuant to Point Section 1.51 / B. 4. in connection with the secondary identifier, then the account holder shall obtain the consent of the entitled person for the assignment of the secondary identifier pursuant to Section 1.51/B.4.

1.51/B.6. The Bank shall ascertain whether the person entitled to dispose over the account is entitled to use the secondary account identifier as such or to modify or delete a notified secondary account identifier. As part of this, the Bank will send a message to the e-mail address to be assigned as secondary identifier requesting a confirmation of a six-digit code from the person authorized to access the e-mail address. In case of mobile phone number, SMS and confirmation. A tax number / tax identification number can be assigned as a secondary identifier if, according to the bank records, the given tax number / tax identification number has already been recorded for that account holder.

1.51/B.7. A 1.51 / B. In the event of failure of the procedure specified in Section 1.51/B.6, the Bank shall refuse to accept the assignment of the secondary identifier or to request the modification or deletion of the submitted secondary identifier.

1.51/B.8. The Bank shall forward the data included in the notification of the person entitled to dispose over the account made in accordance with Point 1.51 / B. 1. herein - - in case of a natural person, on the basis of its consent given pursuant to Point 1.51 / B. 4. - within one hour of completion of the tasks pursuant to point 1.51/B.6. to the central database operator, which shall record it in the central database without delay.

1.51/B.9. The Bank shall process the request to change the reported secondary account ID in accordance with the rules for reporting the secondary account ID.

1.51/B.10. For requesting the deletion of a reported secondary account ID, the Bank shall, within one hour of the completion of paragraph 1.51./B/6, notify the central database management organization, which shall immediately delete it from the central database.

1.51/B.11. The Bank shall reconcile about the validity of the secondary account identifier with the Account Holder or with other person empowered by the Account Holder for the reconciliation annually after receipt of the notification of the person entitled to dispose submitted in line with Point 1.51 / B. in a way that the Bank obtains the confirmation of the person entitled to dispose on the secondary account identifier by the day that is equal to the number of the receipt day. The Bank shall notify the Account Holder of the data reconciliation at least 30 days prior to the expiry of the deadline for annual reconciliation, and shall notify the Account Holder in accordance with Section 1.51 / B. 12.

1.51/B.12. If the data reconciliation does not happen instead of the notification given by the Bank in accordance with 1.51 / B. 11. above within the time specified therein, the secondary account identifier shall expire at 0 am on the day following the expiry of the term, which shall be immediately reported by the Bank to the central database operator, whereby the central database operator shall immediately delete it from the central database.

1.51/B.13. The Bank shall immediately notify the central database operator the termination of the Account Holder's payment account to which it has assigned a secondary account identifier, whereby the central database operator shall immediately delete it from the central database upon receipt of the notification.

Payment request

1.51/C. The Bank currently does not provide any payment request services to its Customers.

FX and international HUF transfers

1.52. It refers to any transfer order whose execution affects at least one currency other than forint, as well as to any HUF transfer orders in which the payment service provider of the beneficiary provides such services outside the boundaries of the Hungary.

FX bank transfers or FX transfers between accounts within the Bank

1.53. Main features of the service: In executing transfers in foreign currency initiated by a Client to the benefit of another client, or transfer orders to be performed between the Client's own accounts, the Bank shall debit the payment account of the paying party and credit the payment account of the beneficiary.

FX and international HUF transfers outside the Bank

1.54. Main features of the service: Transfer orders initiated by the Client shall be forwarded by the Bank to the beneficiary's payment service provider through the settlement mechanisms available to and agreed upon by the Bank, provided to its clients, in compliance with contract provisions and/or general terms and conditions applied by such systems.

1.55. Common rules regarding the data and individual identifiers necessary to execute payment orders:

In FX transfer orders, the Client shall select or enter as a minimum the data to be compulsorily provided in the appropriate fields of the forms or of the order mask available in the electronic banking system. In particular the following data are needed:

Currency of execution / transfer (with a 3-character ISO code),

Amount,

Currency of the amount (with a 3-character ISO code), or if such data are not contained in the order, then the Bank shall consider the currency of execution to be the currency of the amount, as well.

Account to be debited,

Name and address of the paying party,

8- or 11-character BIC (SWIFT) code of the beneficiary's payment service provider – if such code exists, it must be provided.

Name and address of the beneficiary's payment service provider

Beneficiary's account number, in IBAN (International Bank Account Number) format, provided that IBAN account number format exists in the country of the beneficiary.

Name and address of the beneficiary

1.56. If the BIC (SWIFT) code is entered, the Bank performing the order shall consider it as primary information, and disregard the name and address of the beneficiary's payment service provider specified next to the BIC code. If the beneficiary's payment service provider has no BIC (SWIFT) code, the "Bank ID number" usually applied in the given country may also be entered in the appropriate field

of the order. In this case, the bank ID number shall be filled in according to SWIFT standards.

SEPA transfers

- 1.57. Main features of the service: EUR FX transfers (including also intra-Bank EUR transfers), which fall under the scope of Regulation (EU) No 260/2012 of the European Parliament and of the Council on establishing technical and business requirements for credit transfers and direct debits in euro (hereinafter: SEPA Regulation) and thus are to be initiated and performed in a compulsory standardized message format (ISO 20022 XML) along with IBAN account number as payment account identifier (thus without indicating the BIC code). When initiating in electronic form individual EUR transfers, which are not transmitted individually but are bundled together for transmission, the standardised message formats shall be used, provided, that the Clients is neither a consumer nor a microenterprise; in other cases the standardized message format shall be used on the expressed request of the Client only. If possible, Bank shall transmit the SEPA transfer orders marked as urgent via large-value payment system – taking into consideration also Section I. 4.7., –, provided that transferee's payment service provider is available in the large-value payment system.

Collection, and general rules for collection

- 1.58. By submitting a collection order, the Account Owner as beneficiary gives an instruction to the Bank as payment service provider managing its payment account to collect a given amount against the payment account of the paying party, to the benefit of the Account Owner's Payment account.
- 1.59. The collection order shall be submitted by the Account Owner as beneficiary to the Bank as payment service provider managing the Account Owner's Payment account.
- 1.60. After receiving the collection order, the Bank as payment service provider managing the Payment account of the Account Owner as beneficiary shall verify the data relating to the Account Owner as beneficiary (beneficiary according to the document if any document must be attached to the collection order; correspondence between the Account Owner as beneficiary and the Payment account number; signature of the person having rights of disposal as provided to the Bank as payment service provider).
- 1.61. The Bank as payment service provider managing the Payment account of the Account Owner as beneficiary shall forward the data of the collection order to the payment service provider managing the payment account of the

paying party following verification of the items mentioned in section 1.60.

- 1.62. The Bank as payment service provider of the Account Owner as beneficiary may submit the collection order directly to the payment service provider managing the payment account of the paying party.
- 1.63. If any document must be attached to the collection order, or it must be counter-signed based on any provision of law or any agreement, then the collection order so prepared shall be forwarded by the Bank as payment service provider managing the payment account of the Account Owner as beneficiary, and as beneficiary entitled to direct submission according to section 1.60. to the payment service provider managing the payment account of the paying party in a manner enabling the verification of delivery.

Domestic collection

- 1.64. Main general features of the service: Collection orders initiated by the client as beneficiary shall be forwarded by the Bank to the paying party's payment service provider through the settlement mechanisms available to and agreed upon by the Bank, provided to its clients, in compliance with contract provisions and/or general terms and conditions applied by such systems, and/or shall credit the incoming collected amounts to the beneficiary's payment account. In case of domestic collection, payment service providers of both the beneficiary and the paying party shall provide their payment services in the territory of the Hungary.
- 1.65. Common rules for the supply of data and individual identifiers necessary for the execution of collection orders: amount to be collected, Payment account number of the Beneficiary (account to be credited), name of the Beneficiary, Payment account number of the Paying party (account to be debited), name and address of the Paying party, and other compulsory information required for the various sub-types of collection.

Collection based on an authorization letter (type 1)

- 1.66. In the authorization (authorization letter), the account owner as paying party shall authorize the beneficiary – in the manner determined by the account owner at its payment service provider – to submit a collection order. In the authorization letter, the paying party and its payment service provider may also agree upon the conditions of submission.
- 1.67. Compulsory and optional items of the authorization letter, and the order of procedure regarding the termination of Framework Agreements affected by collection transactions

based on authorization letters are governed by the MNB's decree No. 35/2017. (XII. 14.) on cash transactions.

- 1.68. In the absence of the Bank's written confirmation, in the letter authorizing the submission of a collection order, no stipulation regarding the upper limit of the order, the frequency of submission (i.e. occasional, monthly or daily) or its placement in a queue (i.e. keeping in a pending status) shall be valid, and neither shall it be valid to make the withdrawal of the authorization letter dependent on the fulfilment of a particular condition (e.g. consent of a third person). The Bank is entitled to refuse to take receipt of the authorization letter for submitting a prompt collection order if according to the judgment of the Bank the prompt collection orders to be submitted based on the authorization letter may threaten the fulfilment of the Client's payment obligation towards the Bank. Minimum collectable amount shall not be stipulated in the authorization letter, such minimum amounts shall be disregarded by the Bank. In case of collection order based on authorization letter the Bank performs partial payment in all cases, provided that the partially payable amount reaches HUF 100,- or 1 unit of the foreign currency in which the account is managed. The Bank performs partial payment under this amount limit, if the collection order based on authorization letter is fully performed by the partial payment (i. e. in case of the last partial payment).

Collection related to bills of exchange (type 4)

- 1.69. If the collection order is aimed at the collection of claims based on a bill of exchange, the authorization of the direct debtor is represented by the bill of exchange itself.
- 1.70. Detailed rules regarding the submission of the collection order based on bills of exchange as well as the order of procedures for having the bills protested are contained in the MNB's decree No. 35/2017. (XII. 14.) on cash transactions.

Collection order based on an enforceable document according to MNB decree 21/2006 (type 2)

- 1.71. If general conditions of judicial enforcement already existed before 1 November 2009, the obligee may submit a collection order against the obligor's Payment account through a cash transaction to enforce the financial claim even without the respective authorization of the obligor.
- 1.72. If the collection order is submitted based on an enforceable document for the claim to be enforced based on the document serving as a basis for enforcement, the client being an obligee shall state the word "Execution" on the prompt collection order and enter "2" in the field "reason of submission".

- 1.73. To the collection order of type 2, based on an enforceable document, an original or authenticated copy of the document serving as a basis for enforcement shall be attached unless the law provides for otherwise. If the operative part of the decision on appeal serving as a basis for enforcement does not contain the amount of condemnation, the decision of first instance shall also be attached. If enforceability depends on a certain condition or date, a public document certifying the occurrence of that condition or date shall also be attached.

- 1.74. To the collection order submitted to enforce a claim based on a document serving as a basis for enforcement, the obligee shall also attach the statement according to section (1) c) of Article 66 of the Pft. The Bank as payment service provider participating in the execution of the collection order shall not examine whether the statement bears a valid corporate signature.

- 1.75. The obligee may ask for the return of the document serving as a basis for enforcement or the authenticated copy thereof if the document, due to its content, must be used more than one time for the enforcement of claims. The Bank shall execute such orders only if the obligee submits the collection order based on an enforceable document together with the document serving as a basis for enforcement or the authenticated copy thereof and a simple copy (extract) of the operative part of that document.

- 1.76. If the Payment account of the Account Owner as obligor does not provide sufficient coverage for the execution of the collection order based on an enforceable document, and according to the decision attached to the collection order default interest is payable until the date of payment, then the additional interest which the obligee is entitled to for the period of the lack of coverage – in addition to the default interest to be enforced through the collection order – shall be debited to the obligor's Payment account and credited to the obligee's Payment account by the Bank as payment service provider managing the obligor's Payment account acting officially, without any further instruction of the obligee.

Cashing of cheques (type 5)

- 1.77. If the collection order is aimed at the collection of amounts of cheques, the authorization of the issuer of the cheque is represented by the cheque itself. To orders submitted for the cashing of cheques, the original copy of the cheque must be attached.

Direct debit

- 1.78. Based on the authorization given by the Account Owner as paying party concerned, and according to the agreement with its own payment service provider, the beneficiary shall submit collection orders with the same legal titles but to be debited to the payment accounts of different paying parties, bearing a debit date, in the form of batches.
- 1.79. The Bank as payment service provider managing the Payment account of the Account Owner as paying party, based on the authorization received from the Account Owner as paying party for the execution of a direct debit order, shall inform the beneficiary of the acceptance, modification or termination of the authorization through the payment service provider managing the beneficiary's account within six working days from receipt of the authorization. The payment service provider shall only inform the beneficiary of the upper limit of payment with the consent of the Account Owner as paying party. Given that prior to 1 November 2009 the Account Owner is not required to make a statement on the authorization given for a direct debit order about whether the Bank is permitted to inform the beneficiary of the upper limit of payment or not, the Bank shall consider that with respect to authorizations given prior to 1 November 2009 the Account Owner had not authorized the Bank to inform the beneficiary of the upper limit of payments made according to the authorization. If the Client does not complete the section 31 entitled "Statement" of the PFNY specified by MNB's decree No. 35/2017. (XII. 14.), the parties shall consider that the Client did not consent to the notification of the beneficiary on the upper limit of payment.
- 1.80. The beneficiary shall inform the person having contract relations with it as well as the payment service provider managing the account of the paying party on whether it acknowledges or rejects the authorization. The Bank as payment service provider managing the Payment account of the Account Owner as paying party shall consider the authorization as having been acknowledged by the beneficiary also in the event that the beneficiary starts collection.
- 1.81. The authorization as well as the modification thereof may also be sent by the beneficiary to the Bank as payment service provider managing the Payment account of the Account Owner as paying party. The beneficiary shall forward the authorization received from the paying party to the Bank as payment service provider managing the payment account of the paying party. The Bank as payment service provider managing the payment account of the paying party shall handle incoming authorizations as per section 1.79.
- 1.82. Upon request of the Account Owner as paying party, the Bank as payment service provider managing the payment account of the Account Owner as paying party shall issue a certificate on the valid authorization relating to the direct debit order affecting the Payment account of the Account Owner as paying party. Requesting such certificate shall mean no cancellation of the given authorization unless the Account Owner as paying party specifically provides for that. The Account Owner as paying party may submit the certificate to another payment service provider as a new authorization.
- 1.83. Upon taking notice of the new authorization, the beneficiary shall regard the former authorization related to the same agreement as void.
- 1.84. The authorization shall be based on the form PFNY 31 as specified in the MNB's decree No. 35/2017. (XII. 14.) on cash transactions, and the certificate mentioned in section 1.67 shall be based on the form PFNY 31/A as specified in the MNB's decree No. 35/2017. (XII. 14.) on cash transactions.
- 1.85. The beneficiary shall submit the direct debit order at the place, in the manner and with the frequency (deadline of submission) specified in the framework agreement concluded with its payment service provider managing its account at least five working days prior to the debit date stated on the collection order.
- 1.86. The payment service provider of the beneficiary shall perform its tasks arising from the execution of the direct debit order in accordance with section (1) of Article 5 of the MNB's decree No. 35/2017. (XII. 14.) on cash transactions not later than on the working day following receipt of the order.
- 1.87. The Bank may also inform the Account Owner as paying party of the direct debit order prior to the execution thereof.
- 1.88. The Account Owner as paying party may block the execution of the direct debit order with the Bank by the end of the working day preceding the debit date. Blocking may only be effected against the full amount of the collection order affecting the Account Owner as paying party effecting blocking. In case of blocking, the Bank shall proceed according to the instructions related thereto without examining the justification and legitimacy of blocking. Blocking shall not affect the validity and conditions of the authorization.
- 1.89. The Bank as payment service provider managing the payment account of the Account Owner as paying party shall inform the payment service provider managing the

payment account of the beneficiary on the performance or non-performance of the direct debit order as well as on the reasons thereof. The notifications and the data of orders completed shall be forwarded by the payment service provider managing the beneficiary's payment account to the beneficiary in the manner specified in the framework agreement.

1.90. The Bank as payment service provider of the Account Owner as paying party shall inform the paying party of any failed direct debit order not later than upon the subsequent notification provided for in these Terms and Conditions.

1.91. Any direct debit order that cannot be settled due to lack of coverage shall be placed in queue by the Bank until the end of the 3rd Bank Business Day following the value date, and shall be executed according to the original order as soon as coverage becomes available, unless any provision of law provides otherwise.

1.92. The Bank shall effect no partial payment for the direct debit order.

Deferred settlement

1.93. By submitting an order for deferred settlement, the beneficiary gives an instruction to the payment service provider managing its payment account to collect a certain amount from the paying party having an account with the Treasury to the benefit of its own cash account in order to enforce a financial commitment on the basis of an agreement.

1.94. On the order for deferred settlement, the beneficiary shall set a deadline for the paying party to raise objections against performing the payment (hereinafter: deadline for objections). The deadline for objections shall be at the earliest the tenth working day following submission of the order by the beneficiary to the payment service provider managing its cash account.

1.95. Prior to executing an order for deferred settlement, the Treasury shall inform the paying party in advance of the submission of such order, and shall execute the order according to the paying party's instructions. From this point of view, if the paying party does not exercise its right of challenge by the deadline for objections, this shall also be deemed an instruction.

1.96. 1.95. The paying party may lodge an objection with the Treasury against the execution of the order for deferred settlement as a whole or any part thereof at latest by the working day preceding the deadline for objections in the manner and form specified by the Treasury.

1.97. If the paying party raises no objection against the execution of the order for deferred settlement, this shall be deemed a consent to the execution of the collection.

1.98. In case of objection, the Bank shall proceed according to the content thereof without examining the justification and legitimacy of such objection.

Documentary collection

1.99. By submitting an order for documentary collection, the beneficiary of the basic transaction shall hand over the documents serving as a basis for the claim to the payment service provider managing its payment account with the instruction to only deliver them to the paying party (addressee) if payment takes place, the bill of exchange is accepted, or any other conditions are met.

SEPA collection

SEPA collection/debit

1.100. Main general features of the service: The Bank as payment service provider of the obligor shall receive the collection orders submitted against the obligor/ paying party (including also intra-Bank EUR collection orders) in a compulsory standardized message format (ISO 20022 XML) along with IBAN account number as payment account identifier (thus without indicating the BIC code) only if denominated in euro, through the settlement mechanism agreed upon by the Bank, provided to its clients, in compliance with the conditions of the applicable contracts the separate agreement and the SEPA Regulation entered into between the Bank and its clients to the payment service provider of the paying party, shall debit the account of the paying party and shall settle such amounts with the payment service provider of the beneficiary. The Bank is only able to provide SEPA collection services between payment service providers who are members of the SEPA direct debit schemes created by the European Payments Council (EPC) as well as of the system of contracts which regulates it. The Bank as payment service provider of the collector shall not accept or execute SEPA collection orders initiated by the Client as collector/payee.

1.101. When initiating in electronic form individual EUR collections, which are not transmitted individually but are bundled together for transmission, the standardised message formats shall be used, provided, that the Clients is neither a consumer nor a microenterprise; in other cases the standardized message format shall be used on the expressed request of the Client only.

1.102. Common rules regarding the data and individual identifiers necessary to execute SEPA collection orders: Currency of collection – always EUR, Amount, IBAN account number of the collector, name and address of the collector, obligor's IBAN account number, name and address of the obligor, Authorization ID. All further data to be submitted, all formats and conditions related to the method of submission of the order are contained in the separate agreement entered into between the Bank and the collector in connection with the supply of the service.

1.103. Client as payer shall have the right to instruct the Bank (i) to limit a direct debit collection to a certain amount or periodicity or both, (ii) where a mandate under a payment scheme does not provide for the right to a refund, to verify each direct debit transaction, and to check whether the amount and periodicity of the submitted direct debit transaction is equal to the amount and periodicity agreed in the mandate, before debiting their payment account, based on the mandate-related information, (iii) to block any direct debits to the payer's payment account or to block any direct debits initiated by one or more specified payees or to authorise direct debits only initiated by one or more specified payees. With regards to these restrictions the payee's SEPA collection identifier shall serve as payee's identifier.

Core SEPA Direct Debit (hereinafter: CORE SDD)

- 1.104. CORE SDD orders shall not be accepted or executed by the Bank as collector bank.
- 1.105. CORE SDD collection orders shall only be executed by the Bank as obligor bank if it has the Client's preliminary authorization or statement in which the Client declares that he/she wishes to avail of the CORE SDD service, and wants the bank to execute the CORE SDD collection orders submitted against his/her account.
- 1.106. Statements regarding CORE SDD shall only be accepted by the Bank against EUR accounts. The statement shall contain among others the number of the account that shall be debited as a minimum.

Business to Business SEPA Direct Debit (hereinafter: B2B SDD)

- 1.107. B2B SDD orders shall not be accepted or executed by the Bank as collector bank.
- 1.108. B2B SDD orders shall only be executed by the Bank as payer bank based on the Client's preliminary authorization.
- 1.109. Statements regarding B2B SDD shall only be accepted by the Bank against EUR accounts. The statement shall

contain among others the number of the account that shall be debited as a minimum.

1.110. Authorizations for B2B SDD shall only be accepted by the Bank as payer bank from Clients which do not qualify a micro-enterprise or consumer. In case of B2B SDD, the paying party may not exercise its right to reimbursement provided that the Bank acts in compliance with the authorization.

1.111. In case of B2B SDD the Bank shall not be obliged to perform the instructions under Section 1.103.

Payment initiated by the paying party through the beneficiary

1.112. The Bank regulates this method of payment (payment by bank card) in the Bank Card Terms and Conditions.

Documentary credit (letter of credit)

1.113. Within the framework of documentary credit, the payment service provider (opening payment service provider) assumes a liability in its own name, based on the obligor's commission in the basic transaction to pay the beneficiary the amount specified by the letter of credit if the beneficiary submits the required documents to the Bank and such documents are appropriate, or meets certain other conditions prescribed in the letter of credit by a given deadline.

1.114. The beneficiary shall submit the documents specified by the letter of credit to the opening payment service provider directly, by attaching an appropriate letter of request, or through its payment service provider managing its account.

1.115. The opening payment service provider shall pay the amount of documentary credit by bank transfer to the beneficiary's payment account specified by the letter of credit or in the letter of request.

Methods of cash payment related to the Payment account, in particular:

Cash deposit in payment accounts

- 1.116. Cash deposits in a payment account may be accepted by the Bank managing the account, or another payment service provider different from the one managing the account, based on their agreement.
- 1.117. Cash may be deposited at the Bank's cash desk – provided that such service exists in the given Branch – by using a cash deposit form or by signing a cashier's receipt.

1.118. The cash deposit form or the cashier's receipt contains the name and Payment account number of the beneficiary, and makes it possible to enter a reference and other comments allowing for the identification of the paying party by the beneficiary.

1.119. The Bank shall immediately count the money deposited by the Account Owner, and shall immediately makes it available in the Account Owner's Payment account.

Cash disbursement from Payment accounts

1.120. Cashier's disbursement from a payment account means a payment transaction where the Bank pays out cash to the debit of the Account Owner's payment account. The Bank shall execute cashier's disbursement above the sum of HUF 100,000,000 or its countervalue in any currency (calculated with the National Bank's official rate) solely in case a separate agreement between the parties is in effect.

1.121. Cash disbursement by a disbursement postal order means a payment transaction where the Account Owner gives an instruction to the Bank to initiate a HUF disbursement in favour of the beneficiary to the address specified in the order, which the Bank shall perform through postal services.

Methods of payment without Payment account, in particular: Cash transfer

1.122. Cash transfer means a money transfer without the use of a payment account based on a specific agreement, in which the amount transferred is made available to the beneficiary by the Bank a) through disbursement at the Bank's cash desk, or b) by post (postal delivery).
The Bank does not provide FX cash transfer service.

Approval of payment transactions

1.123. The Account Owner as paying party approves the Payment transaction in writing (by signing the payment order or any other document containing approval, and submitting it to the Bank), through Distance Communication or an electronic device. In the latter case, approval shall mean any act or action which, according to the contract provisions related to the given telecommunication or electronic tool (including user guides) means submitting a definitive payment order to the Bank, irrespective of how the given act or action is called in the contract provisions. The approval of the Payment transaction may be done through the Beneficiary or a payment service provider providing Payment Initiation Services.

Arrival and receipt of payment orders

1.124. The Bank shall receive payment orders every Bank Business Day until the closing time defined in the List of Conditions (which shall mean a closing time with respect to the given product and given channel on a working day).

1.125. If any payment order is actually received by the Bank following the closing time of the working day assigned for the receipt of such payment orders, the Bank shall consider it received on the following working day.

1.126. The Bank shall receive payment orders in their order of arrival to the Bank, and shall execute payment orders aimed at the debiting of bank accounts in the order of receipt, unless any provision of law or the Account Owner provides otherwise. The order of receipt shall be established according to the Bank's records. If several payment orders are given at the same time by the Client via Telefonbank, the order of the execution of the payment orders may differ from the reception of such orders. Therefore the Bank and the Client shall agree upon the execution of these orders case by case.

Accepting payment orders

1.127. In case of collection – if the Bank is acting as the service provider of the Account Owner as beneficiary – the time of receiving of the payment order shall be the time where the Bank takes over the payment order along with all data (including identification of the person with rights of disposal) and documents necessary for performing the tasks incumbent upon the Bank.

1.128. In case of collection – if the Bank is acting as the service provider of the Account Owner as paying party – the time of receiving of the payment order shall be the time where the Bank takes over the payment order along with all data and documents necessary for performing the tasks incumbent upon the Bank.

1.129. For cash deposits at the cash desk, the time of receiving of the payment order shall be the time when the Bank takes over the money from the paying party along with all data necessary for the execution in the Bank's premises (branch) used for this purpose.

1.130. For cash deposits made at automatic teller machines enabled for cash deposit, the time of receiving of the payment order shall be the time when the payment service provider verifies the amount deposited, which date may exceed the effective date of deposit by not more than three working days.

- 1.131. For cash disbursement, the time of receiving of the payment order shall be the time when the Bank takes over the payment order along with all data necessary for disbursement, and the financial coverage is available for the payment order to be executed.
- 1.132. Based on an authorisation given by the Account Owner as a paying party in favour of a third person, the Bank shall queue collection orders presented on the basis of such authorisation, as provided in the authorisation. Orders shall only be executed up to the balance available on the account. If the coverage of the payment order is available only in part, the Bank shall execute partially only in the cases specified in the relevant laws and in the case of collection based on authorisation.

Strong Customer Authentication

- 1.132/A. The Bank applies Strong Customer Authentication when the Account Owner as the Paying Party
- a) accesses its Payment Account online,
 - b) initiates a remote electronic payment transaction,
 - c) carries out any action through a remote channel which may imply risk of payment fraud or other abuses.
- 1.132/B. With regard to initiation of electronic payment transactions, the Bank applies Strong Customer Authentication that includes elements which dynamically link the transaction to a specific amount and a specific payee.
- 1.132/C. The Bank applies adequate security measures to protect the confidentiality and integrity of Clients' personalised security credentials.
- 1.132/D. Points 1.132/B and 1.132/C above shall apply where Payment Transactions are initiated through a payment service provider providing Payment Initiation Services.
- 1.132/E. Points 1.132/A and 1.132/C above shall apply where the Account Holder requests the information through a payment service provider providing Account Information Services.

Payment Orders requested by way of using a Payment Initiation Service

- 1.132/F. The Account Holder as a Paying Party shall only be entitled to use Payment Initiation Service, if his Payment Account is online accessible.
- 1.132/G. The Bank shall treat Payment Orders transmitted through the services of payment initiation service provider without any discrimination other than for

objective reasons, in particular in terms of timing, priority or charges vis-à-vis payment orders transmitted directly by the Account Holder as Paying Party. The Bank does not examine the contract between the Account Holder and the third party payment initiation service provider, furthermore, the Bank has no control over the fees charged by the third party provider to the Account Holder, and does not provide information thereof to the Account Holder.

- 1.132/H. In order to use Payment Initiation Services, the Bank has a secure communication connection with the payment service provider providing Payment Initiation Service.
- 1.132/I. After receipt of the Payment Order from the payment service provider providing Payment Initiation Services, the Bank shall immediately provide or make available all information on the initiation of the Payment Transaction and all information – which can be disclosed to the client – accessible to the Bank regarding the execution of the payment transaction to the payment service provider providing Payment Initiation Service.
- 1.132/J. The Bank may deny a payment service provider providing Payment Initiation Services access to a Payment Account for objectively justified and duly proved reasons relating to unauthorized or fraudulent access to the Payment Account by that payment service provider providing Payment Initiation Services, including the unauthorized or fraudulent initiation of payment transactions. In such cases the Bank shall inform the Account Holder that access to the Payment Account is denied and the reasons therefore. That information shall, where possible, be given to the Account Holder before access is denied and at the latest immediately thereafter, unless providing such information would compromise objectively justified security reasons or is prohibited by other relevant Union or national law. The Bank shall allow access to the Payment Account once the reasons for denying access no longer exist. The Bank also denies access to the open API if the TPP's operating certificate is not valid.
- 1.132/K. If the Account Holder makes use of a payment initiation service provided by a Payment Initiation Service Provider, the relevant payment transaction and authorization shall be initiated through the payment service provider performing the Payment Initiation Service. The Payment Initiation Payment Service Provider redirects the Account Holder to one of the Bank's Internet Banking channel which is available on the Bank's homepage (www.unicreditbank.hu) or

through the application of the Bank downloaded to a mobile device where the Account Holder uses the authentication method used there, and the payment order provided by the Payment Initiative Service Provider and its details are displayed on that page. It is only possible to modify the payment order if it is requested by the Account Holder by launching a new authorization through the service provider. After the payment order details are verified by the Account Holder, the payment order is authorized by the usual signing procedure in the bank channel. Information about the submitted payment order can be checked in the given Banking channel. The cancellation of a payment order can also be initiated directly via the bank's channel or through the payment initiation service provider, depending on the service conditions provided by the third party service provider.

Rejecting payment orders

- 1.133. If the payment order does not meet the requirements prescribed by law, the Bank shall refuse to execute it, unless the Bank – exercising its own discretionary powers – executes any payment order issued with data content which does not comply with regulations concerning the issue of such orders to the benefit of the Account Owner submitting the payment order because the Bank is able to ensure compliance with regulations concerning the data content of payment orders without rejecting the given order.
- 1.134. The Bank may reject any payment order which is issued and submitted in a manner not compliant with the conditions set in the framework agreement or in any other agreement concluded with the Account Owner.
- 1.135. Unless otherwise provided for in any legislation, the Bank shall reject payment orders which cannot be executed due to the lack of financial coverage, unless otherwise agreed upon with the Account Owner, in which case the Parties agree that transfer orders shall be put in a queue until the end of the 3rd Bank Business Day following the value date, and shall execute them according to the original order as soon as coverage becomes available.
- 1.136. Payment orders submitted against the Payment account (such as official transfer, transfers based on summons, and prompt collection orders) shall also be executed by the Bank against the credit line related to the bank account.
- 1.137. If the Bank refuses to execute the payment order – unless otherwise provided for by law –, it shall inform the Account Owner of such refusal, and – unless prohibited

by any provision of law – of the reason of refusal if possible, as well as of the procedure to be conducted in order to correct any factual error resulting in the refusal of the order.

Form of payment orders

- 1.138. The Bank is only required to execute payment orders which are received by the Bank through an electronic banking system, through a Payment Initiation Service provider on the form specifically designed by the Bank for this purpose, or on the form specified in MNB's decree No. 35/2017. (XII. 14.) on cash transactions. Payment orders submitted on paper shall be completed by the Account Owner in a legible manner, with black or blue ink pen, or a typewriter or a printer, in a manner to ensure that no addition or other modification of the document nor any forging thereof may be possible, and the document shall also be dated. Following that, the payment order shall in all cases be signed by the person having a right of disposal, in a manner identical to his/her signature provided on the Signature Card.
- 1.139. The Client shall be liable for providing accurate data in a format and with content suitable for the given order type, in compliance with international standards, with intelligible and – in case of hand-writing – legible information. In addition, in case of electronic services it is especially important for the Client to use the appropriate order type and menu item. Failing to do so may result in a delayed or inaccurate transaction, or even the rejection of the order or damages to the client.
- 1.140. Any payment order submitted in a given currency by the person having a right of disposal shall be executed by the Bank against the Account Owner's Payment account maintained in the given currency, unless the person having a right of disposal provides otherwise or it is prohibited by law, and provided that the relevant framework agreement allows for the given payment order to be executed.

Data required for payment orders to be executed

- 1.141. The data necessary for a payment order to be executed are determined in the forms, or – in the case of electronic payment orders – in the data included in the given electronic means of payment.
- 1.142. The Bank shall not accept to execute any document containing a payment order and completed with insufficient, incorrect, unintelligible or inconsistent data, or on which there has been any deletion, modification or correction, or on which the amounts written out in numbers and in letters are not the same, or on which

there has been any addition, deletion or crossing out in the printed content of the document, or which are torn or dirty. In such cases a new form shall be issued.

- 1.143. If the document is intended to be an amendment, confirmation or repetition of a previous payment order, it shall be clearly indicated as such. In the absence of such indication, the Bank shall consider the payment order as a new one.
- 1.144. If the Client has provided incorrect or insufficient data for the order to be executed, the Bank shall not be liable for any damage that arises as a result.
- 1.145. The Bank shall not examine any data entered in the comment field of payment orders, nor their accuracy unless the Bank is required to do so by way of law.

Withdrawal of orders or approvals

- 1.146. The Account Owner as paying party is entitled to withdraw his/her approval given for a payment order by the time specified in this Business Conditions and the List of Conditions. If a joint approval concerning more than one payment transaction is withdrawn, relating future payment transactions shall no longer be deemed approved, either. Upon request, the Bank shall confirm the date of withdrawal to the Account Owner.
- 1.147. Following receipt of the payment order by the Bank, the Account Owner as paying party shall no longer be entitled to withdraw or modify the payment order. If the Payment Transaction is initiated by a payment service provider providing Payment Initiation Service or by or through a beneficiary, the Paying Party shall not be entitled to revoke the Payment Order after giving consent to the payment service provider providing Payment Initiation Service to initiate the Payment Transaction or after giving the Payment Order or consent to execute the Payment Transaction to the beneficiary. In case of collection, the Account Owner as paying party may withdraw the payment order – without prejudice to his/her right to reimbursement – by the working day preceding the debit date. In the case of payment orders with a fixed debit date, the Account Owner may withdraw the payment order by the end of the working day preceding the debit date agreed upon by the Parties.
- 1.148. Following expiry of the above deadline, withdrawal shall be possible in the following cases and by the following deadlines: In the case of payment orders initiated by or through the beneficiary, the withdrawal of the payment order requires the consent of the beneficiary.

- 1.149. If the Account Owner wishes to withdraw his/her approval, he/she shall send the Bank a written statement to this effect by the above deadline. The Account Owner shall reimburse the Bank for any costs incurred in connection with such withdrawal (e.g. cost of change in FX position) upon the first call of the Bank, and the Bank shall be entitled to enforce such claims against the Account Owner's Payment account maintained with the Bank.
- 1.150. The Account Owner shall be liable to the Bank as well as to any other banks participating in transactions for any damages incurred due to payment orders related to the Payment account, or to the data provided therein which are inappropriate, incorrect or insufficient.

Confirmation for the issuers of card-based payment instruments

- 1.150/A. Upon request of the payment service provider issuing the card-based payment instruments – except electronic money – the Bank as the account servicing payment service provider of the Account Holder shall immediately confirm whether an amount necessary for the execution of the card-based payment transaction is available on the payment account of the paying party, provided that all of the following conditions are met:
- a) the payment account of the Account Holder is accessible online at the time of the request,
 - b) the Account Holder has given explicit consent to the Bank to respond to requests from a specific payment service provider to confirm that the amount corresponding to certain card-based payment transaction is available in the payment account,
 - c) the consent stipulated in point b) has been given before the first request for confirmation is made.

The payment service provider issuing the card-based payment instrument may request the confirmation above, if the following conditions are met:

- a) the Account Holder has given explicit consent to the payment service provider to request the confirmation referred to above,
- b) the Account Holder has initiated the card-based payment transaction for the amount in question using a card based payment instrument issued by the payment service provider,
- c) the payment service provider authenticates itself towards the Bank before each confirmation request, and securely communicates with the Bank.

The confirmation

- a) shall consist only in a “yes” or “no” answer and shall not contain a statement of the account balance or the account statement, and shall not be stored or used for purposes other than for the execution of the card-based payment transaction,
- b) shall not allow for the Bank to block funds on the payment account.

The Account Holder shall be entitled to request the Bank to provide information about the name of the payment service provider that requested the confirmation and the content of the such confirmation.

1.150/B. If the Account Holder makes use of a payment service provider issuing a card-based cash substitute payment instrument according to Pft. 38 / A.5 (1), the authorization to do so shall be initiated through the third party service provider. The third party service provider redirects the Account Holder to one of the Bank's Internet Banking channel page which is available on the Bank's homepage (www.unicreditbank.hu) or through the application of the Bank downloaded to a mobile device where the Account Holder uses the authentication method used there, and the authorization given to the third party service provider and its details are displayed on that interface. It is only possible to change the authorization if it is requested by the Account Holder by launching a new authorization through the third party service provider. After the authorization/consent details has been verified by the customer, the authorization is approved in the bank channel. The authorization has no expiry date. The authorization may also be given to one or more payment accounts held by the Account Holder at the Bank. Information about the authorizations can be checked in the given Bank channel. The revocation of the authorization may also be initiated through the third party service provider depending on the service provided by the third party service provider.

Executing payment orders

1.151. When making credit entries, the Bank shall use the account number specified in the payment order. If the HUF amounts to be credited for the benefit of the Account holder should be credited on a Payment account held in other currency than HUF, the conditions applicable to the foreign currency transactions shall be applied. Official transfers and transfers based on summons shall be executed by the Bank also verifying the name and Payment account number of the Account Owner.

1.152. The Bank is entitled to reject credit orders in which the name of the paying party is missing.

1.153. In the case of payment orders given in a currency different from the currency of the Payment account shall be debited or credited in the currency of the Payment account. When performing a conversion between the currency of the Payment account and the other currency, the Bank – unless otherwise agreed upon with the Account Owner – shall apply the exchange rates published by the Bank in the manner specified in these Terms and Conditions.

1.154. The Bank shall credit any Payment account only with amounts which are received by the Bank to the Account Owner's benefit, upon legal titles and in manners permitted by the prevailing legislative provisions. In accordance with legislation on the prevention of money laundering, however, the Bank shall be entitled to examine the origin of any money arriving to the benefit of the Payment account, to request justification for it, and to refuse to credit such amounts in the absence of any appropriate justification. In case of notification of foreign currency or international Hungarian Forint transactions initiated from a different payment service provider and of which the Account Owner is the beneficiary, the Bank may execute the payment transfer prior to the reception of the funds. The Bank retains the right to restore the state of affairs having existed prior to the execution of the payment transfer in case the funds are not received, which means that the Bank may debit the Account Owner's Payment account with the credited amount and the interest, and the Bank shall modify the credit value date to the effective reception of the funds. If the state of affairs having existed prior to the execution of the payment transfer cannot be restored due to the lack of funds on the Account Owner's Payment account, the Bank shall debit any bank account of the Account Owner held with the Bank. The Bank retains the right to execute the payment transfer only after the fact that the funds to the transfer order is received by the Bank.

1.155. Incoming payment orders shall be executed by the Bank according to its List of Conditions.

1.156. Unless otherwise agreed by the Parties, the date of fulfilment of any outgoing payment order shall, in case of domestic payments, be the day on which the beneficiary's Payment account is credited. The order of execution of payment orders shall be contained in the prevailing List of Conditions in which the Bank provides information – among others – as to when the amount of the payment order is likely to be credited to the

beneficiary's bank account, considering the deadline of execution specified in the relevant legal statutes and assuming that all other requirements are met.

- 1.157. With respect to international forint payments (credits and debits), the Bank shall apply the deadlines applicable to the execution of foreign currency payment orders.
- 1.158. In case of Payment Transactions within the EEA, when both the Paying Party and the Beneficiary's payment service provider or the sole payment service provider performing the transaction seated in the territory off the EEA, the Paying Party and the Beneficiary shall only bear the fee, costs and other payment obligations prescribed by their own payment service provider. Also in the case of SEPA payment transactions the Bank shall only accept shared cost bearing method (SHA). Parties agree that in case the payment order does not comply with the above provision, the Bank shall perform the transaction according to the above rule of cost-bearing automatically, without informing the Client or asking for his consent.

Reimbursement

- 1.159.1. Following the request submitted by the Account Owner as paying party within fifty-six days from the debit date, the Bank shall reimburse the amount of the payment transaction initiated by or through the beneficiary and approved by the payer (or shall reject such request by giving an explanation) within ten working days in the following cases:
- a) the Account Owner was not aware of the amount of the payment transaction at the time of approval, and
 - b) the amount of payment transaction exceeded the amount that would have been reasonably expected of the Account Owner in the circumstances, provided that the registered seat of the beneficiary's payment service provider is incorporated in the EEA.
- 1.159.2. A debit transaction shall not be considered as one exceeding the amount that would have been reasonably expected of the Account Owner in the circumstances, if it may reasonably be supposed that,
- a) the amount collected is used to cover a debt arising from a credit or loan agreement between the beneficiary and the Account Owner;
 - b) the Account Owner had determined the maximum amount for the payment transaction, and the amount collected was below that limit unless, notwithstanding the provisions of this paragraph, the Account Owner credibly proves to the Bank the existence of the conditions set forth in paragraph

1.159.1.

- 1.160. When assessing the amount of payment transaction to be reasonably expected of the Account Owner as paying party in the circumstances, the Bank shall take into account the previous payment transactions conducted by the Account Owner as paying party, the provisions of these Terms and Conditions as well as the circumstances of the payment transaction.
- 1.160/A. The refund shall consist the full amount of the executed Payment Transaction. The credit Value Date for the Account Holder as Paying Party shall be no later than the date the amount was debited.
- 1.160/B. The conditions set out in point 1.159 above shall not be fulfilled in case of refund of debits in accordance with Article 1 of the Regulation (EU) No 260/2012 of the European Parliament and of the Council of 14 March 2012 establishing technical and business requirements for credit transfers and direct debits in euro and amending Regulation (EC) No 924/2009.
- 1.160/C. In case of such direct debits denominated in euro, where the payment service provider of both the Paying Party and the Beneficiary, or the sole payment service provider performing the transaction provide their services in the territory of the EEA, the Bank shall not reject the claim of the Paying Party for refund within the time limit prescribed in point 1.159.
- 1.161. If the Account Owner exercises his/her right to reimbursement and wishes to lodge a claim with the Bank for reimbursement regarding the amount collected from him/her, the Account Owner shall attach the following documents to the claim for reimbursement submitted in writing:
- a) the agreement between the Account Owner and the collecting party as beneficiary, making the basis of collection;
 - b) a statement made by the Account Owner being aware of his/her criminal liability, stating that he/she was not aware of the amount of the payment transaction subject to the claim of reimbursement at the time of approving the given payment order;
 - c) the original copies of the invoice and payment information sent to the Account Owner by the collecting party as beneficiary prior to the submission of the claim for reimbursement.
- 1.162. Within 10 working days from the submission of the claim for reimbursement by the Account Owner as paying party (including submission of all documents requested by the Bank), the Bank shall reimburse the

amount of the payment transaction or reject the request by giving an explanation. If, based on the information at its disposal, the Bank decides upon rejecting the claim for reimbursement submitted by the Account Owner as paying party, it shall inform the Account Owner at the same time about the opportunities for the out of court settlement of the dispute as specified in these General Terms and Conditions.

- 1.163. If the Client is not a client qualifying as consumer or micro-enterprise, he/she shall not be entitled to the right to reimbursement specified in the section "Reimbursement".

Correction of payment transactions, rules of liability and allocation of losses

- 1.164. The Account Owner may request the correction of any payment transaction which was not approved or approved but executed incorrectly immediately upon execution of the payment order, but at latest until the day corresponding to the date of debiting of the payment account in the second month (or if the Account Holder is a consumer, in the thirteenth month) following the date of execution of the payment order. If in the month of expiration there is no calendar day corresponding to the date of debiting, the deadline shall expire on the last day of the month. If the Bank has failed to provide the information on the payment transaction subsequently, the time limits determined in this point shall run from the date on which the Bank fulfilled this obligation.
- 1.165. Deleted provision.
- 1.166. If the Account Owner is a client qualifying as consumer or micro-enterprise, in the case of any request of the Paying Party for the correction of payment orders executed without approval or with approval but in an incorrect manner, the Bank shall be obliged to prove – by authentication data if applicable – that the payment transaction subject to complaint had been approved by the Account Owner as paying party, that the payment transaction had been recorded properly, and that execution had not been hindered by any technical problem or disturbance. In case the Payment Transaction requested to correct was initiated by a Payment Initiation Service Provider, the Payment Initiation Service Provider shall be obliged to prove – within its sphere of liability – that the Payment Transaction subject to complaint had been authenticated and recorded properly, and that execution had not been hindered by any technical problem or disturbance of his service.

- 1.166/A. In case of a request of the correction of any payment transaction which was not approved, including, where appropriate, the payment initiation service provider, the use of a payment instrument recorded by the payment service provider shall in itself not necessarily be sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of the obligations under Pft. 40. § (1) and (2). The payment service provider, including, where appropriate, the payment initiation service provider, shall provide supporting evidence to prove fraud or intent or gross negligence fulfilling obligations under Pft. 40. § (1) and (2) on part of the payment service user.

- 1.166/B. In case of an unauthorised payment transaction – regardless whether it was initiated by a payment initiation service provider or not – the payer's payment service provider shall, except where the payer's payment service provider has reasonable grounds for suspecting fraud of the Client and communicates those grounds to the relevant national authority in writing,
- refund the payer the amount of the unauthorised payment transaction immediately, or in any event no later than by the end of the following business day, after noting or being notified of the transaction, and
 - restore the debited payment account to the state in which it would have been had the unauthorised payment transaction not taken place. This shall also ensure that the credit value date for the payer's payment account shall be no later than the date the amount had been debited.

- 1.167. Deleted provision.

Limitation of liability with regard to individual identifier

- 1.168. If the payment transaction is performed using an individual identifier (Payment account number), the payment transaction shall be deemed completed with respect to the beneficiary designated by the individual identifier.
- 1.169. If the execution of any official transfer or transfer based on summons takes place on the basis of an individual identifier, the payment transaction shall be deemed completed with respect to the paying party designated by the individual identifier and the paying party's name.
- 1.170. Should an incorrect individual identifier be used, the Bank shall accept no liability for any non-performance or faulty performance of payment transactions, except the case mentioned in the above section.

1.171. If the Account Owner provides further data in addition to the data and individual identifiers specified by the Bank for the Account Owner as being necessary for the payment order to be executed, the Bank shall be liable for such execution with respect to the individual identifier.

1.171/A. The Bank, as the Paying Party Account Holder's payment service provider shall make all reasonable efforts to recover the funds involved in the Payment transaction. The Bank, as the Beneficiary Account Holder's payment service provider shall cooperate in those efforts also by communicating to the Paying Party's payment service provider all relevant information for the collection of funds. In the event that the collection of funds is not possible, the Bank, as the Paying Party Account Holder's payment service provider shall provide to the Paying Party upon written request, all information available to the Bank and relevant to the Paying Party in order for the Paying Party to file a legal claim to recover the funds.

1.172. Deleted provision.

Liability for the execution of payment transactions

1.173. If the payment transaction was initiated directly by the Account Owner as paying party, the Bank shall be liable for any faulty execution of the payment transaction, unless it can prove that the amount of the payment transaction was received by the beneficiary's payment service provider. If the Bank's liability is ascertained, the Bank shall immediately reimburse the amount of the payment transaction which was not performed correctly or at all to the Account Owner, and shall restore the situation of his/her Payment account as it was before the faulty payment transaction. The credit value date for the Account Holder's payment account shall be no later than the date on which the amount was debited.

1.174. Upon request of the Account Owner as paying party, the Bank – irrespective of the issue of liability for the non-performance or faulty performance of the payment transaction – shall act as it may reasonably be expected in the circumstances regarding the follow-up of any transaction which was not performed correctly or at all, and inform the Account Owner of the results of such follow-up. The Bank shall perform this obligation free of charge for the Account Holder.

1.175. If the payment transaction was initiated by or through the Account Owner as beneficiary, the Bank shall be liable for forwarding the payment order to the payment service provider of the paying party. In case the Bank is

liable under this point, it shall immediately re-transmit the Payment Order in question to the payment service provider of the Paying Party. In the case of a late transmission of the Payment Order, the amount shall be value dated on the Account Holder's Payment Account no later than the date the amount would have been value dated had the transaction been correctly executed.

1.176. The Bank shall be liable to the Account Owner as beneficiary for executing the payment transaction in compliance with legislation. If the Bank's liability is ascertained, it shall be obliged to immediately make the amount of the credit transaction available to the Account Owner in his/her bank account. In this case the amount shall be value dated on the Beneficiary's Payment Account no later than the date the amount would have been value dated had the transaction been correctly executed.

1.177. Subject to the exceptions set out in points 1.175. and 1.176, the Paying Party's payment service provider shall be liable to the payer for non-executed or defectively executed Payment transactions. If the above liability is ascertained, the Bank shall immediately reimburse the amount of the payment transaction which was not performed correctly or at all to the Paying Party, and shall restore the situation of his/her payment account as it was before the faulty payment transaction.

1.177/A. The obligation under point 1.177. shall not apply to the Bank as the Paying Party's payment service provider if the Bank proves that the Beneficiary's payment service provider has received the amount of the Payment Transaction, even if execution of Payment Transaction was delayed. In this case the Beneficiary's payment service provider shall ensure that the value date of the crediting of the amount on the Beneficiary's Payment Account is not later than the date the amount would have been credited had it been executed correctly.

1.178. If the payment transaction was initiated by or through the Account Owner as beneficiary, the Bank – irrespective of the issue of liability for the non-performance or faulty performance of the payment transaction – shall act as it may reasonably be expected in the circumstances regarding the follow-up of the payment transaction, and inform the Account Owner of the results of such follow-up. Fulfilling of the above obligation by the Bank shall be free of charge for the Account Holder.

- 1.179. Provisions of the above sections 1.173 – 1.178 shall only apply if the registered seat of the beneficiary's payment service provider is incorporated in an EEA state.
- 1.180. The Bank shall be liable to the Account Owner for the reimbursement of all fees, costs and other payment obligations incurred in connection with the payment transaction which was not executed correctly or at all by the Bank, as well as for any loss of interest income.
- 1.180/A. If the Payment Transaction was initiated via Payment Initiation Service Provider by the Account Holder as Paying Party, the Bank shall refund the payer the amount of the non-performed or faulty performed payment transaction immediately, or no later than by the end of the following business day, and shall restore the Payment Account to the state in which it would have been had the faulty Payment Transaction not taken place.
- 1.180/E. If the Account Holder uses the account information service of an account information service provider, the concerning authorization shall be initiated through the account information service provider. The Account Information Service Provider redirects the Account Holder to one of the Bank's Internet Banking channel which is available on the Bank's homepage (www.unicreditbank.hu) or through the application of the Bank downloaded to a mobile device where the Account Holder uses the authentication method used there, following which the authorization given to the Account Information Service Provider and its details will be displayed on that interface. It is only possible to modify the authorization if it is requested by the Account Holder by initiating a new authorization through the third party service provider. After the authorization/ consent details has been verified by the Account Holder, the authorization is approved in the bank channel. The authorization shall be valid for a maximum of 90 days from the date of its issuance. The authorization may also be given to one or more payment accounts held by the Account Holder at the Bank. Information about the authorizations can be checked in the given Internet Banking channel. Extension and revocation of the authorization may be initiated through the account information service provider, depending on the service provided by the account information service provider.

Accessibility of Account Information Services

- 1.180/B. The Account Holder as a Paying Party shall only be entitled to use Account Information Service, if his Payment Account is online accessible.
- 1.180/C. In order to use Account Information Services, the Bank has a secure communication connection with the paying service provider providing Account Information Service. The Bank shall treat data requests transmitted through the services of an Account Information Service Provider without any discrimination other than for objective reasons.
- 1.180/D. The Bank may deny a payment service provider providing Payment Information Services access to the Payment Account for objectively justified and duly evidenced reasons relating to unauthorized or fraudulent access to the Payment Account by that payment service provider providing Payment Information Services, including the unauthorized or fraudulent initiation of Payment Transactions. In such cases the Bank shall inform the Account Holder that access to the Payment Account is denied and the reasons therefore. That information shall, where possible, be given to the Account Holder before access is denied and at the latest immediately thereafter, unless providing such information would compromise objectively justified security reasons or is prohibited by other relevant law. The Bank shall allow access to the Payment Account once the reasons for denying access no longer exist. The Bank also denies access to the open API if the TPP's operating certificate is not valid.
- 1.181. Following debiting of the Payment account of the Account Owner as paying party according to the payment order based on the Framework Agreement – unless otherwise agreed or provided for – the Bank shall make available or deliver information concerning payment transactions and the balance of the Payment account once in a month, namely an Account Statement along with the Breakdown of Costs forming an annex thereof to the Account Owner in a manner to enable the Account Owner to store them for a period of time adequate to the purposes of the information and to display them in a format and with a content unchanged. The Bank shall provide the above information free of charge for the Account Holder. The legal effect of the Account Statement shall be identical to the legal effects of the balance of the current account, in other words after the balance of the Payment Account is established by the Bank the Account Owner is only entitled to dispose of the balance of the Payment account and not of the individual claims. The Account Owner shall inform the Bank of his/her potential requests or discrepancies in writing within 30 days from receipt of the information. Omission of the Account Owner to provide such notification shall

Information

be deemed as if he/she agreed with the content of the information and the balancet of the Payment Account.

- 1.182. Upon request of any Account Owner qualifying a consumer, the Bank shall provide the Account Owner qualifying a consumer with the above-mentioned information on paper at least once in a month, free of any fees, charges or any other payment obligations. The Account Owner qualifying a consumer may submit such a request in any Bank Branches or through the Bank's Call Centre during opening hours.
- 1.183. For any Account Owner which is not a client qualifying as consumer or micro-enterprise, the Bank may provide preliminary information in connection with the given payment service by means other than durable medium.
- 1.184. Regarding information to be provided to Account Owners which are not client qualifying as consumer or micro-enterprise, the Bank may deviate from the rules of these Terms and Conditions which it is bound to apply to Account Owners which are client qualifying as consumer or micro-enterprise.

Price of the service, bank charges

- 1.185. The price charged for the service is contained in the List of Conditions.

Amendment of the framework agreement

- 1.186. The Bank shall notify the Account Owner qualifying as consumer or micro-enterprise of its intention to modify the Framework Agreement at least 2 months – in other cases 15 days – before the proposed modification takes effect. The modification shall be deemed accepted by the Account Owner if he/she does not notify the Bank of the contrary before the modification takes effect. This section does not apply to the modification of the reference exchange rate or the reference interest rate.
- 1.186/A. The Client can either accept or reject the amendment of the Framework Agreement before the proposed date of entry into force. In case the Client accepts the amendments, they will entry into force on the proposed date. Rejecting the amendment qualifies as the terminating of the Framework Agreement with immediate effect.
- 1.186/B. In case the amendment terminates any service of the Bank the Parties shall settle up with each other in particular with the fees paid in advance by the Account Owner. In this case the Bank shall charge the pro-rata value of the services actually rendered in accordance

with the Framework Agreement. The settlement shall be free of any charges for the Client.

- 1.187. Until the date preceding the entry into force of the modification, Account Owners which are client qualifying as consumer or micro-enterprise, are entitled to cancel the Framework Agreement with immediate effect, free of any fees, costs or other payment obligations.
- 1.188. If the Client is not a micro-enterprise or a consumer, the Bank is entitled to unilaterally modify the amount of fees and commissions as well as any other contractual provisions without any specific notification, by way of Announcement in the cases set out in the Terms and Conditions for Corporate Clients and Municipalities, and under the terms and by the deadline specified therein.

Termination of the framework agreement and the bank account

- 1.189. The framework agreement shall be terminated (i) upon the Account Owner' death or dissolution without succession; (ii) in case of cancellation, upon expiration of the notice period, in case of cash account in the case specified below.
- 1.189/A. Upon death of the Account Owner, the Framework Agreement shall be terminated (i) in the case of a testamentary order by transferring the account balance to the account of the beneficiary/-ies following their identification and the submission of the certificate of death, or (ii) in other cases, after the identification of the heirs duly proving their rights by an original deed (with an original, final notarial deed of the grant of probate with full effect, a court decision or a certificate of inheritance, or, in the case of foreign persons, the equivalent documents according to the jurisdiction of their respective countries, in an authenticated form) by paying them the amount of the account balance. The Bank shall only deliver the assets, placed with the Bank, of the testator Client holding a Payment account to the heir(s) if the above-mentioned documents are submitted.
- 1.189/B. The Parties shall terminate the framework agreement by mutual consent with immediate effect.
- 1.190. The Account Owner is entitled to cancel the framework agreement without cause in writing, by giving a one-month notice. In this case, the Account Owner shall reimburse all costs incurred by the Bank in connection with termination. The Bank is entitled to cancel the framework agreement without cause in writing, by giving a two-month notice.

- 1.191. If the Account Owner is a client qualifying as consumer or micro-enterprise, any Framework Agreement having been in force for six months or longer may be cancelled by the Account Owner free of any fees, costs and other payment obligations.
- 1.191/A. The Bank shall be entitled to terminate the Framework Agreement and transfer the credit balance of the account to a non-interest bearing suspense account if there has been no activity in the account for a period of at least one year.
- 1.191/B. Expiration of claims in the account shall not automatically result in the termination of the account agreement.
- 1.192. The Bank shall cancel the Cash Account with immediate effect if, within ninety days from opening the cash account, the Bank did not ascertain by a document not older than 30 days issued by the registering organization or by other data that the organization obliged to open a cash account is included in the registry. In this case, the Framework Agreement shall also be terminated, of which the Bank shall inform the Account Owner in writing.
- 1.193. Deleted provision.
- 1.194. Deleted provision.
- 1.195. Deleted provision.
- 1.196. The Framework Agreement can be terminated with immediate effect in the following cases:
- a) the Account Owner – in case of consumer seriously or repeatedly – violates the service agreement or any provisions of the business regulations;
 - b) the Account Owner fails to ensure the conditions specified for the Service to be used;
 - c) the Account Owner does not use the service properly;
 - d) in case of Business Organization: the Account Owner does not fulfil any of his/her payment obligations arising from the service agreement;
in case of consumer: the Account Owner delays any of his/her payment obligations arising from the Service Agreement two times consecutively, and fails to remedy such omission within reasonable deadline specified by the Bank in its payment notice;
 - e) the Account Owner violates copyright in relation to the software;
 - f) the Account Owner attempts to circumvent the security or encryption system of the Service;
 - g) according to the Bank's judgment, any action of the Account Owner in connection with any service is suspected to be a crime, or to be related to a crime.
 - h) if the Client is a consumer a serious breach of contract by the Bank
- 1.196/A. Upon termination with immediate effect, all debts of the Client arising from the Payment account agreement shall immediately become outstanding and payable, and the Client shall settle them with the Bank in a single amount within eight calendar days following receipt of the notice of termination.
- 1.196/B. The Parties shall settle up with each other no later than on the date of termination. In establishing the existence and amount of debts of the Account Owner against the Bank, the Bank's records shall prevail. If the Account Holder uses the cash deposit payment services of the Hungarian Post Ltd., the Account Holder shall inform its clients of the termination of the Payment account and shall arrange the change of those cash deposit payment orders which specifies the Payment account held but terminated with the Bank on time. Amounts arriving after the termination of the Payment account shall be retransferred for the payer through postal services, less the reasonably deducted costs.
- 1.196/C. Upon termination with immediate effect, or if the Client does not give any instructions regarding the amount in the account following termination of the Framework Agreement by cancellation or due to any other reason, the Bank shall transfer the credit balance of the account to a non-interest bearing suspense account for a period of not more than five years.
- 1.196/D. If any Framework Agreement concluded with an Account Owner being a client qualifying as consumer or micro-enterprise is cancelled or terminated, the Bank shall charge the pro-rata value of the service actually rendered in accordance with the Framework Agreement.
- 1.197. **Reimbursement of deposited founders' asset** Provided that the establishment of any corporation or cooperative society fails, the deposited founders' asset shall be refunded by the Bank through repayment to the initial bank account in case of wire transfers or repayment to the founder in case of cash payments; in both cases the costs and fees of the transaction shall be deducted from the funds transferred
- 1.198. **Restriction of the right of disposition over the Payment account**

In case of Clients not qualifying as consumer the Bank shall be entitled to unilaterally restrict the Client's disposition right over its Payment account, as long as due to any reasons emerging on behalf of the Client it cannot be clearly determined who are eligible to act on behalf of the Client or dispose over the Payment account, furthermore provided that the Bank's right to termination with immediate effect can be revoked according to point 1.191, but the Bank either does not intend to exercise its right of termination, or its notice of termination has not yet entered into effect.

1.198/A. Rights of consumers

The Bank shall publish on its website and make available on paper in the customer area of the Bank's premises, at the Bank's agents and at outsourcing service providers the European Commission's leaflet on the rights of consumers under Article 106 (1) of Directive 2015/2366 of the European Parliament and of the Council on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC. The leaflet is also available in an accessible format for persons with disabilities.

2. Opening of deposits

- 2.1. Under a deposit account contract the client is entitled to deposit a specific amount of money to the Bank, and the Bank is obliged to accept the amount offered and to repay the same amount at a later date with interest.
- 2.2. Orders for fixed-term deposits submitted by a Client having a Payment account with the Bank shall be accepted by the Bank from the persons and in the manner specified in the Payment account agreement. The Bank registers the deposit by currencies and by deposit periods in a separate deposit account linked to the bank account, or in the GL account used for registering the deposit.
- 2.3. The Client keeps the amount placed as deposit with the Bank until the date specified in the deposit agreement (time deposit). Cancellation of the time deposit (i.e. withdrawal of deposit) may result in the partial or full loss of the rights to interest payment, and the Bank shall in such case be entitled to call upon the Client to indemnify the Bank for the losses suffered by it. The legal consequences of withdrawing a time deposit are set out in the Bank's prevailing List of Conditions.

- 2.4. The Bank is obliged to make the amount of the deposit placed with it, increased by interests, available to the Client on the maturity date of the deposit.
- 2.5. Unless otherwise provided in the agreement, the Bank shall register depositors that are business organizations by name, registered seat and main activities, and depositors that are natural persons by name, address, place of birth, and ID card (passport) number.
- 2.6. In the prevailing List of Conditions, the Bank shall specify the currencies in which it executes deposit orders submitted on a given day in writing or electronically on the same Bank Business Day as value date. In the case of deposits made in certain currencies, the Bank shall execute the deposit order on the 2nd Bank Business Day following the given day. The Bank shall pay interest on the deposit for the period extending from the opening date until the day before maturity date.
- 2.7. The interest rate payable on the deposit, for the full term of the deposit, shall be equal to the interest rate effective on the opening date.
- 2.8. The Bank calculates the interest payable on deposits as follows:

$$\text{Interest} = \frac{\text{principal} \times \text{interest rate (\%)} \times \text{number of calendar days in the deposit period}}{36\,500}$$

- 2.9. To calculate the average interest rate, the Bank applies the following calculation method:¹

$$\text{Average interest} = \frac{\sum_{i=1}^n (\text{interest rate}_i \times \text{number of days for which the interest rate}_i \text{ is valid})}{\text{number of calendar days in the given period}}$$

- 2.10. Interest on deposits placed with the Bank shall fall due on the day the deposit matures.
- 2.11. If the period remaining until maturity is less than 365 days, the following formula shall be used for calculating the EBKM (unified deposit interest rate ratio):²

$$\text{Deposit made} = \sum_{i=1}^n \frac{(k+bv)i}{1+r \times (t_i / 365)}$$

¹ where n is the number of changes in interests during the given period

² where
n is the number of interest disbursements,
r is one hundredth of the EBKM,
t_i is the number of days remaining from the opening date until the ith disbursement,
(k+bv)i is the sum of the principal and interest paid back upon the ith disbursement.

- 2.12. If the period remaining until maturity is 365 days or more, the following formula shall be used for calculating the EBKM:³

$$\text{Deposit made} = \sum_{i=1}^n \frac{(k+bv)i}{1+r^{(t_i/365)}}$$

- 2.13. If the deposit is made in more than one instalment, the following formula shall be used for calculating the EBKM:⁴

$$\sum_{i=1}^n \frac{B_i}{(1+r)^{(t_i/365)}} = \sum_{j=1}^m \frac{K_j}{(1+r)^{(t_j/365)}}$$

- 2.14. The Bank shall inform its depositor Clients about any changes to the EBKM by modifying its List of Conditions and by publishing them in the form of announcements.
- 2.15. The minimum amount in which forint and foreign currency deposits may be opened are specified by the Bank's List of Conditions. From corporate clients, the Bank accepts deposit orders in HUF rounded up to hundred thousands, and in foreign currency rounded up to thousands, except for deposits with automatic renewal.
- 2.16. The shortest period of deposit – depending on the clientele and the currency – is contained in the prevailing List of Conditions.
- 2.17. The Client may request the term of deposit to be extended, in the case of deposits made in a currency specified in the List of Conditions not later than on the Bank Business Day being the maturity date of the deposit, and in the case of other currencies not later than two Bank Business Days before the maturity date of the deposit. The Bank shall establish a new deposit interest rate for the extended period, which shall be equal to the one applicable to newly opened deposits.
- 2.18. In the case of orders given for the opening of a deposit with automatic renewal – unless otherwise provided for by the Client – the Bank shall, on each maturity date, renew the

time deposit for the term specified in the original order. Each time the deposit is renewed it shall be considered a new time deposit, and thus the Bank shall determine a new interest rate for each term, taking into account the reference interest rate specified in the agreement. If the Client wishes to cancel the order for the deposit with automatic renewal, the deadlines stipulated in section III.2.16. for the submission of the statement of cancellation shall apply. In the event of a continuous deposit, the Bank may make additional deposit modification orders permitting regular or minimum deposit balances for the day of the deposit, the availability of which may be restricted by the Bank to certain account types or channels as specified in the Bank's Announcements.

- 2.19. With respect to time deposits opened for a specific purpose, the parties shall sign a separate agreement.
- 2.20. The Bank shall not deduct any costs or fees from the amount of interest payable to the Client for the deposit. Exceptions to this are items that must be deducted according to the law.
- 2.21. Conditions pertaining to the withdrawal of the deposit prior to maturity, the Uniform Deposit Interest Rate Ratio (EBKM), as well as all facts and information that have an effect on the amount payable prior to or upon maturity, are contained in the Bank's List of Conditions. The Bank shall pay interest on the currencies listed in the List of Conditions.
- 2.22. Unless otherwise provided for by the Hpt. regarding deposit insurance, deposits placed with the Bank are – within the scope and to the extent specified by the Hpt. – insured by the National Deposit Insurance Fund (OBA). Insurance provided by the Fund does not cover the following:
Deposits made by:

(1)

- a) any publicly financed institution,
- b) any business organization which is fully owned by the State on a permanent basis,
- c) any local government,
- d) any insurer, reinsurance company, voluntary mutual insurance fund or mandatory pension fund,
- e) any investment fund or investment fund manager,
- f) any Pension Insurance Fund as well as the institutions managing them; administrative bodies for pension insurance,
- g) allocated public funds,
- h) any financial institution, payment service provider
- i) the National Bank of Hungary,

³ where
n is the number of interest disbursements,
r is one hundredth of the EBKM,
t_i is the number of days remaining from the opening date until the ith disbursement,
(k+bv)i is the sum of the principal and interest paid back upon the ith disbursement.

⁴ where
n is the number of deposit instalments,
B_i is the amount of the ith deposit instalment,
t_i is the number of days remaining from the date of first instalment until the date of the ith instalment,
r is the rate of EBKM,
m is the number of disbursements,
t_j is the number of days remaining from the opening date until the date of the jth instalment,
K_j is the amount of the jth disbursement.

- j) any investment firm, member of the stock exchange, or commodity exchange service provider,
- k) mandatory or voluntary deposit insurance, institutional insurance or investors protection fund, and the Private Pensions Guarantee Fund,
- l) any risk capital organization or risk capital fund nor the deposits made by any equivalent of the above institutions in foreign countries.

(2)

- a) deposits for which the court established by a final judgment that the amount deposited had been earned through money laundering,
- b) to the own funds of credit institutions and debt securities issued by credit institutions and promissory notes.

By way of derogation from 2.22 (1) a) and c) points, the insurance provided by OBA shall cover the accounts of local governments and the accounts of budgetary agencies set up by local governments, if the local government's budgetary balance sheet total shown in the financial report prepared for the year two years prior to the given year does not exceed five hundred thousand euro. The amount of this five hundred thousand euro limit shall be translated to forints by the official exchange rate published by the MNB acting within its central banking duties, in effect on the last day of the year two years prior to the given year.

- 2.23. If the Client of the Bank holding a deposit account dies, for one year after the grant of probate or the judgement adopted in the inheritance proceedings steps into effect or until the expiry of the fixed-rate interest period - whichever occurs later - the deposit granted or provided to the heir in the judgment shall be transferred by the Bank in the interest of the heir to the technical account of the heir (sub account) connected to the Payment account of the heir (main account) held at the Bank, if the heir wishes the Bank to transfer this amount to an account held at the Bank or to be deposited at that account. The reason for the above is that this way the Bank can take into account this deposit as a separate amount separated from other deposits of the heir when establishing the indemnification amount guaranteed by the National Deposit Insurance Fund. Compensation for the testator's deposit shall be payable up to the amount guaranteed by the National Deposit Insurance Fund, regardless of the number of heirs. If the testator has Discretionary Account opened for the eligibility for the higher indemnification amount according to Section 2.24. the heirs will be entitled for the higher indemnification amount for 3 months after the grant of probate or the judgement adopted in the inheritance proceedings steps

into effect regardless of the number of heirs.

This technical account is a restricted account, no transfers can be made to this account except the deposit of the decedent, no money can be transferred or paid to this account either. Payment orders can be made for the amount of the technical account. The official transfers and transfers based on summons against the main account will be executed against the balance of the technical account too. The heir takes into account that if the technical account is charged under any legal title the amount of the charge will be deducted from the deposit of the decedent thus the indemnification amount guaranteed by the National Deposit Insurance Fund will be decreased with the amount of the charge. The technical account will be terminated after one year of the grant of probate or the judgement adopted in the inheritance proceedings steps into effect, without any further legal actions, and the positive account balance of the account will be automatically transferred to the Payment account of the heir (main account). If the main account is terminated for any reason, the subaccount is also terminated. The bank will not charge any additional charges and fees for the upkeep of the subaccount in addition to the charges and fees of the main account.

- 2.24. Upon the Client's request the Bank register the deposit of the Client to be handled separately on a discretionary account opened to the benefit of the Client (Discretionary Account) so that the National Deposit Insurance Fund is able to provide a further maximum EUR 50,000 indemnification amount, in addition to the general maximum EUR 100,000 indemnification amount, to natural person, sole trader and small-scale agricultural producer Clients holding deposits at the Bank as follows:

- 2.24.1. As a requisite for the separation of the deposit, thus the eligibility for the higher indemnification amount, the Client shall provide the Bank with a trustworthy evidence that the deposit originates from the following sources:
- a) the sale of residential property, or the sale of lease rights or any right of tenancy;
 - b) benefits received upon the termination of employment or upon retirement;
 - c) insurance benefits; or
 - d) compensation received for criminal injuries or wrongful conviction.
- 2.24.2. The Client is entitled to certify the source of the separated deposit on the day the deposit was opened at the Bank with the following documents in cases defined in Section a) of 2.24.1. the copy of the contract

on the sale of residential property or other document on the transfer of property, lease rights or the rights of tenancy not older than 30 days;
 in cases defined in Section b) of 2.24.1. certificate of the employer or payer not older than 30 days;
 in cases defined in Section c) of 2.24.1. certificate of the insurance company not older than 30 days;
 in cases defined in Section d) of 2.24.1. decision of the court not older than 30 days.

2.24.3. The Discretionary Account is a technical, restricted account connected to the Payment account of the Client. No deposit originating from other sources shall be placed to this account. After the deposit was separated no money can be transferred or paid to this account either. The official transfers and transfers based on summons against the Payment Account will be executed by the Bank against the balance of the technical account. However no other payment orders can be made for the amount of the Discretionary Account, save for the transfer of the separated deposit to the Payment Account of the Client.

2.24.4. The Discretionary Account is terminated without any further legal actions at the latest three months after it was opened. With the termination the positive balance of the Discretionary Account will be automatically transferred to the Payment Account of the Client. The Discretionary Account is terminated without any further legal actions if the separated deposit is terminated. If the Payment Account is terminated for any reason the Discretionary Account is terminated simultaneously.

2.24.5. The Bank will not charge any additional charges and fees for the upkeep of the Discretionary Account in addition to the charges and fees of the Payment Account

2.25. In case of deposits insured by the National Deposit Insurance Fund offsetting between the Bank and the Client will be possible if the Client owes an overdue unpaid amount to the Bank expired before the opening day of the compensation procedure

2.26. Detailed information on important matters regarding the National Deposit Insurance Fund – such as deposit types covered, extent of insurance, conditions for the payment of indemnity, and order of procedure for indemnification – can be obtained from the prevailing information material available in branches and on the Bank's website.

3. Collection of postal fee for postal cash services

- 3.1. The Bank undertakes to arrange for payments through Magyar Posta Zrt. for postal cash payment orders initiated by the Client, if the Client ensures coverage for the costs of the order and the related postal fee in his/her bank account. Upon submission of the postal cash payment order, the Bank debits the Client's account with the fee charged by the Post as well as with the amount of the order based on the instruction. The Bank undertakes to credit the Client's Payment account with the amount of cash payment in relation to local cash services provided by the Post, and to transfer data between the Client and the Post. The Bank debits the Client's Payment account with the postal fee of the local cash service, where the value date is the due date appearing on the invoice sent by the Post.
- 3.2. For postal cash services, the Bank shall charge the Client a fee as per the List of Conditions, under the terms specified therein. Furthermore, the Bank shall also debit the Client's Payment account with the fee(s) charged by Magyar Posta Zrt.

4. Cheque

- 4.1. Cheque shall mean any instrument bearing the formal characteristics set out in the decree of the Ministry of Justice No. 2/1965. (I.24.).
- 4.2. Valid and authentic cheques issued in the form prescribed by the prevailing legislation shall be cashed by the Bank at its own discretion, i.e. the Bank shall buy them or take them over from the Client for collection. The Bank takes over cheques in HUF in domestic circulation only for the purpose of collection. If the Bank paid the amount of cheque to the Client in advance, and the cheque is not be paid upon presentation, the Bank shall be entitled to debit the Client with the amount paid or the claim arising from the Bank's right to reimbursement.
- 4.3. The Bank purchases the cheque at a price defined in the prevailing List of Conditions. The cheque – depending on the type – shall be settled by disbursement at the cash desk or by crediting the Client's Payment account maintained with the Bank.
- 4.4. The Bank is entitled to charge the Client with the commission and the costs incurred in connection with cheque cashing in the currency of the cheque's counter-value and to deduct this amount from the counter-value of the cheque.

- 4.5. The Bank is entitled – by drawing up a record – to withdraw any cheques which, according to the Bank's information, have been stolen or lost or if there is a suspicion that they are forged or counterfeit.

5. Foreign currency trading

- 5.1. Unless otherwise agreed upon the Bank concludes foreign currency exchange transactions only with a Client maintaining an account with the Bank.
- 5.2. The Bank purchases or sells currencies and foreign currencies at an exchange rate defined by the Bank, under the conditions set in the List of Conditions or in an individual agreement. The Bank does not set exchange rates for the following currencies and does not undertake to serve the cash management for these currencies: RUB, HKD, PLN, RON, TRY, CNY, RSD.
- 5.3. Foreign currency trading transactions at a so-called market price shall only be concluded over the phone or through the "UC Trader" system, for which a treasury framework agreement, a framework contract for spot FX conversion transactions or a "UC Trader" agreement respectively must be concluded with the Bank. Trading over the phone or through the "UC Trader" system may only take place under the terms and conditions of the respective agreement. The method of identifying the Client is described in the respective agreement.
- 5.4. The Bank shall record phone conversations regarding the FX trading agreement between the Client and the Bank as well as any relevant information supply, and the Bank is entitled to use the recorded phone conversations as evidence in case of disputes. Failing proof to the contrary, the records shall certify the content of phone conversations. The Client shall solely be liable for any damages incurred by either the Bank or the Client due to any trading conducted by unauthorized persons on behalf of the Client.
- 5.5. If the Bank executes the instructions of the Client in performing FX trading transactions, the full profit or loss generated in the Client's position shall belong to the Client. In the case of Clients who are natural persons, the Bank shall pay the Client the profit reduced by the appropriate amount of advance tax payment according to tax legislation.

6. Custody service

Within the framework of its custody service, the Bank shall place and handle any amount defined by the Client in an interest-bearing or non-interest-bearing separated custody account under the conditions set out by relevant legislation. Detailed conditions regarding custody services are contained in the custody agreement concluded with the Client and in the Bank's prevailing List of Conditions.

7. Safe service

- 7.1. Based on the agreement concluded with the Client, the Bank shall make a safe available to the Client in premises under continuous surveillance; the Client shall place valuables in the safe and take them out of there on his/her own.
- 7.2. The Bank shall only conclude any safe deposit agreement by performing client vetting. In this case, the Client shall also make a statement to the Bank to specify whether he/she is acting in his/her own name and interest, or on behalf of and in the interest of the actual owner according to Pmt.
- 7.3. The Bank shall insure the valuables placed in the safe up to an amount set in the agreement to be concluded with the Client – but up to a maximum per safe as set in the List of Conditions relating to safe deposit – against a fee specified in the List of Conditions.

8. Credit reference service

Upon request or authorization of the Client put in a public document or in a private document providing full evidence, the Bank shall provide third parties with banking information about the Client within the scope of bank secret specified in the said document and without violating the bank secret, against a fee specified in the prevailing List of Conditions or in the individual agreement.

9. Brokerage of financial services

The Bank conducts brokerage activities solely for financial institutions or bank group clients in order to support their deposit-taking, lending and other service providing activities under the conditions set out in the individual agreement concluded with the Client.

10. Currency exchange

- 10.1. The Bank exchanges currencies during the opening hours of the Bank's cash desk, based on the Bank's buying or selling rates of exchange as specified by the Bank in the exchange rate table displayed.
- 10.2. The Bank shall withdraw any currency that seems to be forged or counterfeit – by drawing up a record thereof – and send it to MNB immediately for the purpose of investigation.
- 10.3. The receipt of such money – whether prior to the conclusion of the investigation or when MNB ascertains that the money is forged or counterfeit and withdraws it from circulation – shall not give rise to any financial claim on the part of the Client.

11. EFER service

- 11.1. The Client may perform his payment obligations towards institutions participating in Electronic Payment and Settlement System (EFER) electronically, via the Bank's EFER service. The conditions and method of payment via EFER are specified by regulations and other information (www.magyarorszag.hu).
- 11.2. To be able to use the Bank's EFER service, the Client shall have a HUF Payment Account and an adherent Spectra, SpectraNet Internet Banking and/or SpectraNet Mobile Banking service with the Bank.
- 11.3. The Client shall initiate the EFER payment transaction at the beneficiary institution participating in EFER. Payment orders shall be submitted to the Bank indicating the EFER payment identification number specified by the beneficiary institution.
- 11.4. Data of the payment order registered in EFER – including validity period and payment identification number – is forwarded to the Bank by EFER itself. The Bank insures that the payment order with the registered data (hereinafter: EFER payment order) is available immediately for the

Client in the Spectra, SpectraNet Internet Banking and/or SpectraNet Mobile Banking service.

- 11.5. After checking the data of the EFER payment order displayed by Spectra, SpectraNet Internet Banking and/or SpectraNet Mobile Banking service, the Client may accept (i.e. submit) the payment order or refuse it. It is not possible to change the data of the EFER payment order in such services – except for the value date of execution which may not be later than the last day of the validity period.
- 11.6. The EFER payment order is executed only against HUF Payment Account, fees and other costs defined for EFER service will be charged. The Bank shall execute EFER payment orders only if the financial coverage necessary is available on the account to be debited according to the EFER payment order. The Bank places the EFER payment order in a queue until the end of the validity period. The Bank shall not perform partial payment for the EFER payment order.
- 11.7. The EFER payment order shall be accepted or refused within its validity period. Payment orders that are not accepted within the validity period shall not be executed and will be deleted automatically from the Bank's system.
- 11.8. The Bank shall send a verification to EFER of the EFER payment orders which have been accepted, refused – by duly signing and submitting to the Bank – or deleted due to the expiry of the validity period.
- 11.9. The Bank shall bear no responsibility for the damages arising in connection with EFER payment orders which have been refused or not accepted within the validity period by the Client or which have not been executed by the Bank in compliance with the rules regulating EFER payment orders.
- 11.10. Hereinafter, rules set forth for electronic domestic transfer orders shall be applicable to EFER payment orders.

IV. EFFECT OF THE GENERAL TERMS AND CONDITIONS

The consolidated text of the General Terms and Conditions shall come into effect on 10th December 2020 – with the exceptions below – for an indefinite period of time.

- (1) The modifications relating to the Private Invest Application of subsection 2.26. of Part I. and sections 1.1.–1.5.4., and 5.1 – 5.5.6. of Part II. shall enter into force on 1 January 2021.

In case of any discrepancies between the Hungarian text of the General Terms and Conditions and the present English text, the Hungarian version shall prevail.

Budapest, 22nd September 2020

UniCredit Bank Hungary Zrt.

ANNEX 1.

OUTSOURCED ACTIVITIES

Within the framework of outsourced activities:

1. securities account statements are printed, placed in envelopes and posted by EPDB Nyomtatási Központ Zrt. (registered seat: H-1117 Budapest, Budafoki út. 107-109.);
2. storage and management of documents as well as other related services are provided by Iron Mountain Kft. (registered seat: H-1093 Budapest, Czuczor utca 10.);
3. production and personalization of blank cards and pin envelopes, personalization of bank cards, and pin envelopes, packing and posting of cards, pin envelopes and different items sent in envelopes are carried out by THALES DIS Deutschland GmbH (Werinherstrasse 81, 81541 München, Germany);
4. production of basic materials necessary for the personalized issue of credit card account statements (hereinafter: account statements) and items sent to clients; ensuring the intact condition and checking the volume of PDF extract files submitted; personalization of account statements and client mailings based on the PDF extract files sent; production of basic materials necessary for the personalized issue of payment account statements (hereinafter: account statements) and client mailings; development of the list file generating programs based on the data set transferred and the layout, in the case of a layout modification requirement, the alteration of the programs; with the approved list file generating programs, generation of the list files needed for personalization based on the data set transferred; personalization of account statements and client mailings based on the list files generated; putting into envelope the personalized account statements and client mails; preparation of letters for posting; and delivery of the letters prepared for posting to Magyar Posta Zrt's OLK office in Budaörs are carried out by EPDB Nyomtatási Központ Zrt. (H-1117 Budapest, Budafoki út. 107-109.)
5. all IT development and operation services necessary for the performance of the activities of UniCredit Bank Hungary Zrt. are provided by UniCredit Services S.C.p.A ("US") (Italy, I-20151 Milano, Via Livio Cambi 1.);
6. the administration and operation of the system used for providing target balancing services (cash management/ CPE/ instrument) are carried out by UniCredit Bank AG. (Kardinal-Faulhaber-Str. 1, DE-80333 Munich, Germany);
7. under the CSA (Credit Support Annex) agreements concluded with the clients of the Bank, collateral management based on the current market value of live derivative transactions is carried out by UniCredit Bank Austria AG (Schottengasse 6-8., A-1010 Vienna, Austria).
8. activities relating to dispute resolution and portfolio reconciliation as set out by Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories are provided by UniCredit Bank Austria AG (Schottengasse 6-8., 1010 Vienna, Austria).
9. activities relating collection, transportation and destruction of documents supposed to be destructed are provided by Iron Mountain Kft. (registered seat: H-1093 Budapest, Czuczor utca 10.).
10. communication services supporting CRM activities are provided by NeoSoft Informatikai Szolgáltató Kft. (8000 Székesfehérvár, Távírda utca 2/A.).
11. IT software and interface development services, software customization and implementation services, project management, and IT consultancy services in connection with development services, necessary for the performance of the activities of UniCredit Bank Hungary Zrt. are provided by UniCredit Business Integrated Solutions Austria GmbH (1090 Vienna, Nordbergstrasse 13).
12. IT application services for Payment Account Switch are provided by GIRO Elszámolásforgalmi Zártkörűen Működő Részvénytársaság (1054 Budapest, Vadász u. 31.)
13. translating, lectorating and interpreting services are provided by Afford Fordító- és Tolmácsiroda Kft. (1093 Budapest, Lónyay utca 29.).
14. translating, lectorating and interpreting services are provided by InterContact Budapest Kft. (1054 Budapest, Hold u. 15.).
15. translating, lectorating and interpreting services are provided by Interlingo Bt. (1026 Budapest, Pasaréti út 47.).

16. cash and valuables transfer service, money processing service, security of the outsourced security depository, "Intelligent Trezor" service, ATM operation service are provided by Criterion Készpénzlogisztikai Korlátolt Felelősségű Társaság (1139 Budapest, Rozsnyai u. 21–25.).
17. e-firm gate service is provided by e-Jogsegéd Szolgáltató Korlátolt Felelősségű Társaság (1135 Budapest, Kisgömb utca 6/1.)
18. interpreting services are provided by Interlex Communications Kft. (1013 Budapest, Attila út 33.)
19. data warehouse developing services regarding HITREG project are provided by BSCE Tanácsadó és Informatikai Kft. (Magyarország, 1134 Budapest, Róbert Károly körút 82-84.)
20. Alipay acceptance service as part of the POS Bankcard acceptance service is provided by Ingenico Hungary Kft. (1134 Budapest, Váci út 19.).
21. card issuing, POS and ATM acquiring services are provided by SIA Slovakia a.s. (Einsteinova 25, 851 01 Bratislava, Slovakia) and SIA Central Europe a.s. Magyarországi Fióktelepe (1117 Budapest, Alíz utca 4.).
22. customer experience/customer satisfaction survey services are provided by MaritzCX GmbH (22765 Hamburg, Borselstrasse 18., Germany)

ANNEX 2.

DATA CONTROLLING GUIDELINES

I. Data controlling guidelines

Definitions

‘processing’: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

data transfer: ensuring access to the data for a predetermined third party.

data processing: performing technical tasks in connection with data processing operations, irrespective of the method and means used for executing the operations, as well as the place of execution, provided that the technical task is performed on the data.

data subject: any natural person directly or indirectly identified or identifiable by reference to specific personal data.

sensitive data: personal data revealing racial or ethnic origin, political opinion, religion or beliefs, trade union membership, as well as genetic data, biometric data used for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation

profiling: means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements

personal data: any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical,

physiological, genetic, mental, economic, cultural or social identity of that natural person.

Data controller

The data controller is UniCredit Bank Hungary Zrt. (registered seat: 1054 Budapest, Szabadság tér 5-6., website: www.unicreditbank.hu, (hereinafter: Bank).

Purpose of processing

The purpose of data processing is the particular reason for which the collection, processing and controlling personal data is necessary. The purposes of the data processing cases implemented by the Bank are set out in section II of this Annex.

Processed personal data

The personal data processed by the Bank are set out in section II of this Annex.

Legal basis for processing

The Bank processes personal data only if data processing has a legal basis, that is, if

- a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes,
- b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract,
- c) processing is necessary for compliance with a legal obligation to which the Bank is subject,
- d) processing is necessary in order to protect the vital interests of the data subject or of another natural person,
- e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Bank,
- f) processing is necessary for the purposes of the legitimate interests pursued by the Bank or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The legal bases for the data processing cases implemented by the Bank are set out in section II of this Annex.

Duration of data processing

The Bank processes personal data only for the period needed for achieving the purpose of processing, taking into account the statutory requirements regarding duration of processing.

The duration of the data processing cases implemented by the Bank is specified in section II of this Annex.

Processing of personal data for other purposes

Where the Bank intends to process the data subject's personal data for a purpose other than that for which they were collected – unless such purpose derives from a statutory provision – the Bank

- a) shall ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected,
- b) and shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information.

Rights of the data subject

The Bank shall ensure enforcement of the following rights granted to data subjects, also cooperating with the data subjects in exercising their rights:

- a) **right to information:**
the Bank shall – in line with the principle of fair and transparent data processing – provide the data subject, in compliance with the statutory regulations, with the information stipulated by law,
- b) **right of access:**
the data subject shall have the right to obtain from the Bank confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the information specified by law. The Bank shall provide the data subject with a copy of the personal data undergoing processing. For any further copies requested by the data subject, the Bank may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form,
- c) **right to withdraw a consent:**
if the legal basis for data processing is the data subject's consent, then data subject shall have the right to withdraw his or her consent at any time, although the withdrawal

of consent shall not affect the lawfulness of processing based on consent before its withdrawal. After the consent has been withdrawn, the Bank may still process personal data in order to fulfill its legal obligations or to enforce its legitimate interests, provided that the interest enforcement is commensurate with the restriction on the right to personal data protection.

- d) **right to rectification:**
the data subject shall have the right to obtain from the Bank without undue delay the rectification of inaccurate personal data concerning him or her, and to have incomplete personal data completed,
- e) **right to erasure:**
the data subject shall have the right to obtain from the Bank the erasure of personal data concerning him or her without undue delay, which request may only be rejected in the cases stipulated by law, particularly if data processing is required for compliance with a legal obligation in Union or Member State law to which the Bank is subject, or if this is necessary for the establishment, exercise or defence of legal claims. If the data processing is stipulated by law, the Bank may not erase the data subject's data.
- f) **right to be forgotten:**
this right requires that, where the Bank has made the personal data public and is obliged, pursuant to the right to erasure, to erase the personal data, then the Bank, taking account of available technology and the cost of implementation, shall take reasonable steps (including technical measures) to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.
- g) **right to restriction:**
the data subject shall have the right to obtain from the Bank restriction of processing, if
 - the accuracy of the personal data is contested by the data subject (for a period enabling the Bank to verify the accuracy of the personal data),
 - the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead,
 - the Bank no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims, or
 - the data subject objects to the processing, exercising his or her right to object (pending the verification whether the legitimate grounds of the Bank override those of the data subject),
- h) **right to information on recipients who are notified of the rectification or erasure of personal data or restriction of processing:**

the Bank shall communicate any rectification or erasure of personal data or restriction of processing carried out at the data subject's request to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The Bank shall inform the data subject about those recipients if the data subject requests it.

i) **right to data portability:**

if the legal basis for data processing is the data subject's consent or the performance of the contract, and processing is carried out by automated means, the data subject shall have the right to

- receive the personal data concerning him or her, which he or she has provided to the Bank, in a structured, commonly used and machine-readable format,
- and have the right to transmit those data to another controller without hindrance from the Bank,
- and, if technically feasible, they may request that their personal data be transferred directly between data controllers,

j) **right to object:**

The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data necessary in the Bank's or a third party's legitimate interest, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Bank, including profiling. The Bank shall no longer process the personal data unless the Bank demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. If the Bank processes personal data for direct marketing purposes (including profiling), then, in case of the data subject's objection, the personal data may no longer be processed for such purposes. The Bank agrees that the data subject shall have the right to object to his or her personal data for direct marketing purposes, at any time and free of charge,

k) **the data subject's right not to be subject to a decision based solely on automated processing:**

the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. This right shall not be granted to the data subject if the decision:

- is authorised by Union or Member State law to which the Bank is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests,
- is necessary for entering into, or performance of, a contract between the data subject and the Bank,
- is based on the data subject's explicit consent.

In the latter two cases the Bank shall grant the data

subject the right to obtain human intervention on the part of the Bank, to express his or her point of view and to contest the decision

l) **rights related to audio recordings:**

the data subject may request that the audio-recorded phone conversation be replayed or a copy of it be provided to him or her, or, if the object of the conversation is a complaint, the issue of a certified report on the audio-recording.

m) **restriction or prohibition of data transfers within the bank group:**

the data subject may, by means of an explicit statement, at any time restrict or prohibit data transfer within the bank group (under Section 164/B of the Credit Institutions Act)

n) **right to judicial remedy:**

- o) if the data subject considers that his or her personal data is controlled in breach of the statutory requirements, he or she may file a complaint with a data protection supervisory authority or seek effective judicial remedy. The data subject has the opportunity to contact the Bank's data protection officer before submitting the complaint or referring the matter to the court, and to inform him or her of the problem regarding the Bank's data processing.

Method of submitting the data subject's requests

The data subject may submit his or her requests related to processing

- by post, to the UniCredit Bank Hungary Zrt. 1242 Budapest Pf. 386 address,
- electronically, to the panasza@unicreditgroup.hu e-mail address,
- by phone, on the +36(1/20/30/70) 325-3200 telephone number,
- personally, at the Bank's branch offices

Handling of the data subject's requests

The Bank shall inform the data subject of the action taken in response to his or her request within one month of receipt of the request submitted by the data subject. This deadline may be extended by two further months. The Bank shall inform the data subject of any such deadline extension within one month of receipt of the request, together with the reasons for the delay.

Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

If the Bank does not take action on the request of the data subject, the Bank shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

Automated decision-making, profiling

The Bank may use automated decision-making to assess creditworthiness against pre-defined criteria. In this case, prior to the conclusion of a loan (credit) contract, the Bank will use the personal data of the data subject in an automated decision-making process (including profiling), in a simplified, scoring-based rating (evaluation) system.

In relation to this, the data subject may

- a) request human intervention,
- b) express his or her point of view,
- c) challenge the decision.

Parties entitled to access data

The employees and agents of the Bank and of any other data controllers and data processors may access data to the extent required for the performance of the functions within their job responsibilities.

Recipients of the personal data

Recipients of the personal data are the data controller's agents and data processors. The parties involved in transferring personal data are listed in section III of these Data controlling guidelines.

Data processors

In relation to data processing, the Bank may use the services of a data processor. In this case the data processor performs processing on the Bank's behalf.

The Bank shall use only data processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the statutory requirements and ensure the protection of the rights of the data subject. The processor shall not engage another processor without prior specific or general written authorisation of the Bank. The data processor listed in section IV of these Data controlling guidelines.

The latest list of the data processors and the tasks performed by them will later be available on the www.unicreditbank.hu website and in the information notice available in the Bank's branches.

Data transfer within the bank group: (Section 164/B of the Hpt.)

The Bank and the financial institutions, payment institutions, electronic money institutions, investment firms, insurance companies, AIFMs and UCITS managers they control shall be allowed to exchange the personal data of clients they process, data classified as bank secrets, securities secrets, payment secrets and insurance secrets, and data classified as business secrets to the extent required in connection with their operations and for the provision of their services, in accordance with the standard contract terms of the data processors participating in such shared data processing, and they shall be permitted to transmit such data directly with a view to allowing access to their individual services, and to process the data thus received during the time period for setting up and during the existence of client relationships.

With regard to the Bank and other companies controlled by it, accessing and processing the data referred to above shall be allowed only to companies

- a) such that are pursuing activities:
 - aa) aiming to promote non-cash digital payment services and to provide consumers with such payment methods,
 - ab) aiming to introduce digital applications to support the management of parties who are not consumers,
 - ac) working to improve the financial awareness of consumers and to introduce digital financial means to them,

and

- b) data processing is performed in the interest of setting up client relations in that context of services.

The current list of companies controlled by the Bank is as follows:

- UniCredit Jelzálogbank Zrt.
- UniCredit Leasing Hungary Zrt.

The client may, based on an express declaration, at any time restrict or prohibit the data transfer described above. Such declaration can be made

- by post, to the UniCredit Bank Hungary Zrt. 1054 Budapest, Szabadság tér 5-6 address,
- electronically, to the info@unicreditgroup.hu e-mail address,
- by phone, on the +36(1/20/30/70) 325-3200 telephone number,
- personally, at the Bank's branch offices.

Data protection

The Bank protects the controlled personal data by means of technical and organisational measures against unauthorised

access, alteration, transfer, public disclosure, deletion or destruction, as well as damage and accidental loss, and ensures that the stored data cannot be corrupted and rendered inaccessible due to any changes in or modification of the applied technique.

For the protection of data sets stored in its different electronic filing systems, the Bank will introduce suitable technical solutions to prevent, unless this is permitted by law, the interconnection of data stored in these filing systems and the identification of the data subjects.

Liability, restitution

The Bank shall be liable for any damages caused to a data subject as a result of unlawful processing or by any breach of data security requirements, and, provided that the infringement has been recognised or established with legally binding effect, it shall pay compensation for damages. In the event of violation of the data subject's personality rights, the data subject may claim restitution (Section 2:52 of the Civil Code). The Bank shall also be liable for damage caused by the data processor whose services it is using. The Bank shall also bear liability for damages caused by a controller that is in a joint controller relationship with the Bank.

The Bank shall be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

Possibility for seeking judicial remedy or lodging a complaint

Regarding lawfulness of data processing, the data subject can initiate a procedure with the National Authority For Data Protection and Freedom of Information (1125 Budapest, Szilágyi Erzsébet fasor 22/c., postal address: 1534 Budapest, Pf.: 843, website: www.naih.hu, tel.: +36 (1) 391-1400, fax: +36 (1) 391-1410, central e-mail: ugyfelszolgalat@naih.hu) or he/she may take the matter to the court competent in the region where the Bank's head office or his or her (permanent or temporary) residence is located.

We recommend that you contact our data protection officer before turning to the National Authority for Data Protection and Freedom of Information or to the court.

Contact details of the data protection officer

Contact details of the Bank's data protection officer:

- by post, to the UniCredit Bank Hungary Zrt. 1054 Budapest, Szabadság tér 5-6 address,
- electronically, to the adatvedelmitisztviselo@unicreditgroup.hu e-mail address,

II. Purposes of processing, legal bases, processed personal data, duration of data processing

Data processing cases

- A) Data processing related to the provision of financial services
 - A/1. New loan or new credit card application, loan administration, risk analysis and assessment, avoidance of future losses to the Bank
 - A/2. Provision of credit and cash loans
 - A/3. Financial administration of special schemes (e.g. state-subsidised loans, employer loans)
 - A/4. Taking deposits and receiving other repayable funds from the public, in excess of equity
 - A/5. Provision of payment services
 - A/6. Commercial activities in foreign currency, foreign exchange, other than currency exchange services, bills of exchange and cheques on own account or as commission agents
 - A/7. Provision of sureties and bank guarantees, or the assumption of other bankers' obligations.
 - A/8. Provision of safe custody service and safe deposit box service
 - A/9. Issuance of paper-based cash substitute payment instruments (e.g. paper-based traveller's cheques, bills of exchange) or provision of services related thereto that are not classified as payment services;
 - A/10. Intermediation of financial services, and intermediation of insurance under the terms provided for in the Act on Insurance Companies and the Insurance Business
 - A/11. Credit pre-screening where initiated, information about credit options and contacting the inquirer about credit options and credit pre-screening using the contact details provided in the case of telephone inquiries
- B) Provision of auxiliary financial services
 - B/12. Currency exchange activity
- C) Investment and auxiliary investment services, and other services provided by the Bank on a professional basis
 - C/13. Securities lending, nominee activities, investment services, services auxiliary to investment services, and intermediation and activities available to commodity dealers under Sections 111 to 116 of the Investment Services Act.

- C/14. Enabling the account holder to gain information on the actual data of the securities account and the customer account on the website of the National Bank of Hungary.
- D) Other processing cases
- D/15. Market research, opinion polls, client satisfaction surveys
- D/16. Direct marketing, data controlling for marketing purposes, season's greetings, communication with individuals who use specific channels to inquire about the Bank's products
- D/17. Customer relations, arrangements for events, ongoing efforts to maintain data accuracy, complaints management, receivables management, other operational customer services
- D/18. Performance of the Agreement between the Government of Hungary and the Government of the United States of America to Improve International Tax Compliance and to Implement the FATCA
- D/19. Audio-recordings produced in the Bank's call center and other similar customer service / relevant sales areas operating on similar principles
- D/20. Monitoring, for property protection and security purposes, of entry to and exit from specific buildings and premises used by the Bank
- D/21. Production and retention of video recordings made, for the protection of confidential securities and business information, security, and the protection of human life and physical integrity, of natural persons intending to enter, for specific purposes, to the Bank's seat and establishments and other buildings used by the Bank as private areas open to the public
- D/22. Data controlling regarding to consumer clients of UniCredit Leasing Hungary Zrt.

Abbreviations

Taxation Act: Act CL of 2017 on Tax Administration Procedure

Investment Services Act: CXXXVIII of 2007 on Investment Firms and Commodity Dealers, and on the Regulations Governing Their Activities

GDPR: 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)

FATCA Act: Act XIX of 2014 on the promulgation of the Agreement between the Government of Hungary and the Government of the United States of America to Improve International Tax Compliance and to Implement FATCA and on the amendment of other related acts

Credit Institutions Act: Act CCXXXVII of 2013 on Credit Institutions and Financial Enterprises, CCIS Act: Act CXXII of 2011 on the Central Credit Information System

Act on Personal Data: Act LXVI of 1992 on the Registration of the Personal Data and Address of Citizens
AML Act: Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing

Personal Income Tax Act: Act CXVII of 1995 on Personal Income Tax

Accounting Act: Act C of 2000 on Accounting

Security and Investigators Act: Act CXXXIII of 2005 on Security Services and the Activities of Private Investigators

	Purpose of processing	Legal basis for processing	Processed personal data	Duration of data processing (erasure of data)
A) Data processing related to the provision of financial services				
A/1	New credit card application, loan administration, risk analysis and assessment, avoidance of future losses to the Bank			
1.	risk assessment related to the evaluation of credit card applications	the Bank's legitimate interest	bank account number, details of the loan application (purpose and type of the loan, term, type of interest charged, loan amount, details of the housing loan, subsidies and preferential terms granted), details of the combined loan, personal data (name, birth name, place and date of birth, in case of mortgage loans the personal identification number, mother's birth name, residence, ownership of residence, mailing address, marital status, level of schooling), credit card data, the applicant's income and other details (confirmed regular monthly net income, other confirmed regular monthly income, regular monthly spending of the household, number of earners and dependent members in the household, type of legal relationship underlying the incomes), the loan applicant's regular financial commitments and debts, details of the collateral property (address, title number, type of property, means of construction, estimated market value)	in the case of loss of purpose/interest or successful objection, or a failed contract conclusion, the time that the claim related to the failed contract conclusion becomes enforceable
2.	risk assessment related to the evaluation of credit card applications	consent	in case of application/contracting with biometric signature, the biometric data made available to the Bank with the signature on the sign pad	in the case of loss of purpose or withdrawal of consent, or a failed contract conclusion, the time that the claim related to the failed contract conclusion becomes enforceable
3.	conclusion or performance of credit card contract	performance of contract	bank account number, details of the loan application (purpose and type of the loan, term, type of interest charged, loan amount, details of the housing loan, subsidies and preferential terms granted), details of the combined loan, personal data (name, birth name, place and date of birth, in case of mortgage loans the personal identification number, mother's birth name, residence, ownership of residence, mailing address, marital status, level of schooling), credit card data	the contract's limitation period
4.	conclusion or performance of credit card contract	consent	in case of contracting with biometric signature, the biometric data made available to the Bank with the signature on the sign pad	the contract's limitation period
5.	conclusion or performance of credit card contract	the Bank's legitimate interest	the applicant's income and other details (confirmed regular monthly net income, other confirmed regular monthly income, regular monthly spending of the household, number of earners and dependent members in the household, type of legal relationship underlying the incomes), the loan applicant's regular financial commitments and debts, details of the collateral property (address, title number, type of property, means of construction, estimated market value), mobile phone number	loss of purpose/interest, or successful objection
6.	the client's identification in relation to a credit card contract	statutory obligation (AML Act)	family name and first name, family name and first name of birth, nationality, place and date of birth, mother's birth name, address of residence, or (in the absence of such) temporary residence, type and number of identification document, politically exposed person status	8 years from the termination of the business relationship or the execution of the transaction order
7.	identification of beneficial owner in relation to a credit or loan agreement	statutory obligation (AML Act)	family name and first name, family name and first name of birth, nationality, place and date of birth, address of residence, or (in the absence of such) temporary residence, politically exposed person status	8 years from the termination of the business relationship or the execution of the transaction order
8.	verifying the authenticity and appropriateness of the personal data provided through the GRIInfo system	consent	name, address of residence, mother's name, number of identification document, photograph, signature	the contract's limitation period
9.	fulfilment of the obligation to retain accounting documents	statutory obligation (Accounting Act)	data in the accounting document	8 years
10.	non-postal liaison	consent	e-mail address, phone number	withdrawal of consent / contract limitation period

	Purpose of processing	Legal basis for processing	Processed personal data	Duration of data processing (erasure of data)
A) Data processing related to the provision of financial services				
A/2	Provision of credit and cash loans			
1.	risk assessment related to the evaluation of credit and loan applications	the Bank's legitimate interest	name, signature, name at birth, mother's birth name, place and date of birth, nationality, address of residence, ownership of residence, mailing address, in the case of mortgage loans the personal identification number, sex, marital status, legal status for currency purposes, politically exposed person status, fact of legal capacity, number of personal identity card (passport), number of other identification appropriate for identifying a person under the Act on Personal Data, in the absence of an address of residence the address of temporary residence; highest level of schooling, employer (including the place of work where different), position, income and method of payment (e.g. wire transfer), any garnishments (including reasons and amounts); sector of employment, (previous) employment relationship (including the beginning and end of the period of notice), term and type of entrepreneurship, participation in any undertaking from which income is derived, date of occupation of current residence; number of persons in the household, number of children under 14 in the household; net monthly income of partner or spouse, unconfirmed net monthly income, monthly spending, other (securities, cash, deposits), income and other details of the household (such as incapacity for work); names and positions of authorised representatives of legal persons and entities lacking the status of a legal person, identification data, as specified in the foregoing, of the agent for service of process and collateral provider, if a natural person, and those of other natural persons involved in the credit assessment, monthly net income of any joint and several guarantors living in the same household; type of mobile phone (such as pre- or postpaid, company or private), data on the customer's rating for work-out purposes	in the case of loss of purpose/interest or successful objection, or a failed contract conclusion, the time that the claim related to the failed contract conclusion becomes enforceable
2.	risk assessment related to the evaluation of credit and loan applications	consent	in case of application / contracting with biometric signature, the biometric data made available to the Bank with the signature on the sign pad	in the case of loss of purpose or withdrawal of consent, or a failed contract conclusion, the time that the claim related to the failed contract conclusion becomes enforceable
3.	conclusion or performance of credit or loan contract	performance of contract	name, signature, name at birth, mother's birth name, place and date of birth, nationality, address of residence, ownership of residence, mailing address, in the case of mortgage loans the personal identification number, sex, marital status, legal status for currency purposes, fact of legal capacity, number of personal identity card (passport), number of other identification appropriate for identifying a person under the Act on Personal Data, in the absence of an address of residence the address of temporary residence; names and positions of authorised representatives of legal persons and entities lacking the status of a legal person, identification data, as specified in the foregoing, of the agent for service of process and collateral provider and other natural persons involved in the credit assessment	the contract's limitation period
4.	conclusion or performance of credit or loan contract	consent	in case of application / contracting with biometric signature, the biometric data made available to the Bank with the signature on the sign pad	withdrawal of consent / contract limitation period
5.	conclusion or performance of credit or loan contract	the Bank's legitimate interest	highest level of schooling, employer (including the place of work where different), position, income and method of payment (e.g. wire transfer), any garnishments (including reasons and amounts); sector of employment, (previous) employment relationship (including the beginning and end of the period of notice), term and type of entrepreneurship, participation in any undertaking from which income is derived, date of occupation of current residence; number of persons in the household, number of children under 14 in the household; net monthly income of partner or spouse, unconfirmed net monthly income, monthly spending, other (securities, cash, deposits), income and other details of the household (such as incapacity for work); monthly net income of any joint and several guarantors living in the same household; type of mobile phone (such as pre- or postpaid, company or private), data on the customer's rating for work-out purposes	loss of purpose/interest, or successful objection

	Purpose of processing	Legal basis for processing	Processed personal data	Duration of data processing (erasure of data)
A) Data processing related to the provision of financial services				
A/2	Provision of credit and cash loans			
6.	conclusion or performance of credit or loan contract	statutory obligation (Taxation Act, Personal Income Tax Act)	Tax ID number	contract limitation period / until the expiry of the right to tax determination
7.	identification of customer in relation to a credit or loan agreement	statutory obligation (AML Act)	family name and first name, family name and first name of birth, nationality, place and date of birth, mother's birth name, address of residence, or (in the absence of such) temporary residence, type and number of identification document, politically exposed person status	8 years from the termination of the business relationship or the execution of the transaction order
8.	identification of beneficial owner in relation to a credit or loan agreement	statutory obligation (AML Act)	family name and first name, family name and first name of birth, nationality, place and date of birth, address of residence, or (in the absence of such) temporary residence, politically exposed person status	8 years from the termination of the business relationship or the execution of the transaction order
9.	providing for a more robust assessment of creditworthiness, and supporting the fulfilment of the conditions for responsible lending and reducing the credit risk, as well as the security of debtors and reference data providers through the Central Credit Information System	statutory obligation (CCIS Act)	name, name at birth, place and date of birth, mother's birth name, number of personal identity card (passport), or the number of any another document suitable for verifying identity under the Act on Personal Data, address of residence, mailing address, e-mail address, contract data defined in the CCIS	the term specified in the CCIS Act (10 years in case of termination of contractual relationship or failed repayment, or, if the debt has been settled, 1 year following settlement, or 5 years, in case of fraud)
10.	in the context of the preliminary risk assessment required for the conclusion of the contract, the receipt of the data specified in the CCIS Act from the financial firm managing the CCIS.	consent (As per the CCIS Act)	name, name at birth, place and date of birth, mother's birth name, number of personal identity card (passport), or the number of any another document suitable for verifying identity under the Act on Personal Data, address of residence, mailing address, e-mail address, contract data defined in the CCIS	withdrawal of consent or termination of the contractual relationship
11.	verifying the authenticity and appropriateness of the personal data provided through the GIRinfo system	consent	name, address of residence, mother's name, number of identification document, photograph, signature	withdrawal of consent / contract limitation period
12.	fulfilment of the obligation to retain accounting documents	statutory obligation (Accounting Act)	data in the accounting document	8 years
13.	non-postal liaison	consent	e-mail address, phone number	withdrawal of consent / contract limitation period

	Purpose of processing	Legal basis for processing	Processed personal data	Duration of data processing (erasure of data)
A) Data processing related to the provision of financial services				
A/3	Financial administration of special schemes (e.g. state-subsidised loans, employer loans)			
1.	risk assessment related to the evaluation of credit and loan applications	the Bank's legitimate interest	name, signature, name at birth, mother's birth name, place and date of birth, nationality, address of residence, mailing address, personal identification number, sex, marital status, legal status for currency purposes, fact of legal capacity, number of personal identity card (passport), number of other identification appropriate for identifying a person under the Act on Personal Data, in the case of foreign nationals the address of residence in Hungary; highest level of schooling, employer, position, income; sector of employment, (previous) employment relationship, term and type of entrepreneurship, participation in any undertaking from which income is derived, date of occupation of current residence; number of persons in the household, number of children under 14 in the household; net monthly income of partner or spouse, unconfirmed net monthly income, monthly spending, other (securities, cash, deposits); names and positions of authorised representatives of legal persons and entities lacking the status of a legal person, identification data, as specified in the foregoing, of the agent for service of process and collateral provider, if a natural person, and those of other natural persons involved in the credit assessment	in the case of loss of purpose/interest or successful objection, or a failed contract conclusion, the time that the claim related to the failed contract conclusion becomes enforceable
2.	risk assessment related to the evaluation of credit and loan applications	consent	in case of application / contracting with biometric signature, the biometric data made available to the Bank with the signature on the sign pad	in the case of loss of purpose or withdrawal of consent, or a failed contract conclusion, the time that the claim related to the failed contract conclusion becomes enforceable
3.	conclusion or performance of credit or loan contract	performance of the contract / statutory obligation [Taxation Act, Personal Income Tax Act, Gov. Decree 16/2016. (II. 10.), Gov. Decree 17/2016. (II. 10.)]	name, signature, name at birth, mother's birth name, place and date of birth, nationality, address of residence, mailing address, tax ID number, personal identification number, sex, marital status, legal status for currency purposes, fact of legal capacity, number of personal identity card (passport), number of other identification appropriate for identifying a person under the Act on Personal Data, in the case of a foreign national the address of residence in Hungary; names and positions of authorised representatives of legal persons and entities lacking the status of a legal person, identification data, as specified in the foregoing, of the agent for service of process and collateral provider and other natural persons involved in the credit assessment	the contract's limitation period
4.	conclusion or performance of credit or loan contract	consent	in case of application / contracting with biometric signature, the biometric data made available to the Bank with the signature on the sign pad	withdrawal of consent / contract limitation period
5.	conclusion or performance of credit or loan contract	the Bank's legitimate interest	highest level of schooling, employer, position, income, sector of employment, (previous) employment relationship, term and type of entrepreneurship, participation in any undertaking from which income is derived, date of occupation of current residence; number of persons in the household, number of children under 14 in the household; net monthly income of partner or spouse, unconfirmed net monthly income, monthly spending, other (securities, cash, deposits)	loss of purpose/interest, or successful objection
6.	identification of customer in relation to a credit or loan agreement	statutory obligation (AML Act)	family name and first name, family name and first name of birth, nationality, place and date of birth, mother's birth name, address of residence, or (in the absence of such) temporary residence, type and number of identification document, politically exposed person status	8 years from the termination of the business relationship or the execution of the transaction order

	Purpose of processing	Legal basis for processing	Processed personal data	Duration of data processing (erasure of data)
A) Data processing related to the provision of financial services				
A/3	Financial administration of special schemes (e.g. state-subsidised loans, employer loans)			
7.	identification of beneficial owner in relation to a credit or loan agreement	statutory obligation (AML Act)	family name and first name, family name and first name of birth, nationality, place and date of birth, address of residence, or (in the absence of such) temporary residence, politically exposed person status	8 years from the termination of the business relationship or the execution of the transaction order
8.	providing for a more robust assessment of creditworthiness, and supporting the fulfilment of the conditions for responsible lending and reducing the credit risk, as well as the security of debtors and reference data providers through the Central Credit Information System	statutory obligation (CCIS Act)	name, name at birth, place and date of birth, mother's birth name, number of personal identity card (passport), or the number of any another document suitable for verifying identity under the Act on Personal Data, address of residence, mailing address, e-mail address, contract data defined in the CCIS	the term specified in the CCIS Act (10 years in case of termination of contractual relationship or failed repayment, or, if the debt has been settled, 1 year following settlement, or 5 years, in case of fraud)
9.	in the context of the preliminary risk assessment required for the conclusion of the contract, the receipt of the data specified in the CCIS Act from the financial firm managing the CCIS	consent (as per the CCIS Act)	name, name at birth, place and date of birth, mother's birth name, number of personal identity card (passport), or the number of any another document suitable for verifying identity under the Act on Personal Data, address of residence, mailing address, e-mail address, contract data defined in the CCIS	withdrawal of consent or termination of the contractual relationship
10.	fulfilment of the obligation to retain accounting documents	statutory obligation (Accounting Act)	data in the accounting document	8 years
11.	establishing entitlement to family housing allowance, and checking lawfulness of use	consent	the data determined in Government Decree 16/2016. (II. 10.) on housing-purpose state subsidies for the construction and purchase of new homes, and Government Decree No. 17/2016 (II. 10.) on the Family Housing Allowance for the Resale or Extension of Used Homes	until withdrawal of consent, or period required for establishing entitlement to family housing allowance, and checking lawfulness of use
12.	examination of the tax-free nature of the employer's housing allowance, issue of a certificate of disbursement of the employer's housing allowance	consent	name, name at birth, place and date of birth, mother's birth name, tax ID number, the data defined in Decree 15/2014 (IV.3.) of the Ministry for National Economy on the rules of payment of tax free employer housing subsidy	withdrawal of consent or termination of the contractual relationship
13.	fulfilment of the obligation to retain accounting documents	statutory obligation (Accounting Act)	data in the accounting document	8 years
14.	non-postal liaison	consent	e-mail address, phone number	withdrawal of consent / contract limitation period

	Purpose of processing	Legal basis for processing	Processed personal data	Duration of data processing (erasure of data)
A) Data processing related to the provision of financial services				
A/4	Taking deposits and receiving other repayable funds from the public, in excess of equity			
1.	conclusion or performance of contract related to placement of deposits and other repayable funds	performance of contract	name, name at birth, mother's birth name, place and date of birth, nationality, address of residence, mailing address, number of personal identity card (passport), number of other identification appropriate for identifying a person under the Act on Personal Data, in the absence of an address of residence the address of temporary residence; politically exposed person status; names and positions of authorised representatives of legal persons and entities lacking the status of a legal person, identification data of the natural person agent for service of process; personal data of the beneficiary relevant to the nature of the investment service, as specified in the foregoing	the contract's limitation period
2.	conclusion or performance of contract related to placement of deposits and other repayable funds	consent	in case of application / contracting with biometric signature, the biometric data made available to the Bank with the signature on the sign pad	withdrawal of consent / contract limitation period
3.	customer's identification in relation to a contract related to placement of deposits and other repayable funds	statutory obligation (AML Act)	family name and first name, family name and first name of birth, nationality, place and date of birth, mother's birth name, address of residence, or (in the absence of such) temporary residence, type and number of identification document, politically exposed person status	8 years from the termination of the business relationship or the execution of the transaction order
4.	beneficiary owner's identification in relation to a contract related to placement of deposits and other repayable funds	statutory obligation (AML Act)	family name and first name, family name and first name of birth, nationality, place and date of birth, address of residence, or (in the absence of such) temporary residence, politically exposed person status	8 years from the termination of the business relationship or the execution of the transaction order
5.	fulfilment of the obligation to retain accounting documents	statutory obligation (Accounting Act)	data in the accounting document	8 years
6.	non-postal liaison	consent	e-mail address	withdrawal of consent / contract limitation period

	Purpose of processing	Legal basis for processing	Processed personal data	Duration of data processing (erasure of data)
A) Data processing related to the provision of financial services				
A/5	Provision of payment services			
1.	conclusion or performance of contract for provision of payment services	performance of contract	name (e.g. cardholder's name, name on the card, in relation to cash withdrawal / deposit the name of the person performing the transaction, names of clients, beneficiaries and collectors of transfers and collections), name at birth, mother's name, place and date of birth, type and number of personal identification document, social security ID number, nationality, permanent address, mailing address, marital status, personal identification data, as listed above, of persons living at the same permanent address of residence, address card number, name(s) of the owner(s) of POS/VPOS trading organisations, natural person trader's name; name, position, contact data (phone, fax) of contact persons in the retail premises, data (e.g. card number, expiry) required for executing card transactions (e.g. authorisation); account number of clients, beneficiaries and collectors of transfers and collections, personal data indicated in the notes or authorisation letters, in the case of bill-of-exchange collection, the personal data indicated on the bill of exchange	the contract's limitation period
2.	conclusion or performance of contract for provision of payment services	the Bank's legitimate interest	place of work (employer), organisational unit, position, start of employment, mobil phone	loss of purpose/interest, or successful objection
3.	conclusion or performance of contract for provision of payment services	consent	in case of application / contracting with biometric signature, the biometric data made available to the Bank with the signature on the sign pad	withdrawal of consent / contract limitation period
4.	conclusion or performance of contract for provision of payment services	statutory obligation (Taxation Act, Personal Income Tax Act)	Tax ID number	contract limitation period / until the expiry of the right to tax determination
5.	customer identification related to contracts for provision of payment services	statutory obligation (AML Act)	family name and first name, family name and first name of birth, nationality, place and date of birth, mother's birth name, address of residence, or (in the absence of such) temporary residence, type and number of identification document, politically exposed person status	8 years from the termination of the business relationship or the execution of the transaction order
6.	beneficial owner's identification related to contracts for provision of payment services	statutory obligation (AML Act)	family name and first name, family name and first name of birth, nationality, place and date of birth, address of residence, or (in the absence of such) temporary residence, politically exposed person status	8 years from the termination of the business relationship or the execution of the transaction order
7.	Ensuring withdrawal of cash, free of any fee or charge, by means of cash-substitute payment instruments, from an automated teller machine located in Hungary	performance of contract	name, name at birth, place and date of birth, mother's birth name, payment account number	the contract's limitation period
8.	fulfilment of the obligation to retain accounting documents	statutory obligation (Accounting Act)	data in the accounting document	8 years
9.	non-postal liaison	consent	e-mail address, phone number	withdrawal of consent / contract limitation period
10.	Data transmit to Third-Party Provider (TPP)	performance of a contract	Account information (account details, balance, transactions), payment order details	Revocation of authorization to a Third Party Provider or termination of performance of contract for provision of payment services

	Purpose of processing	Legal basis for processing	Processed personal data	Duration of data processing (erasure of data)
A) Data processing related to the provision of financial services				
A/6	Commercial activities in foreign currency, foreign exchange, other than currency exchange services, bills of exchange and cheques on own account or as commission agents			
1.	trading in foreign currency, foreign exchange (other than currency exchange services)	performance of contract	name, address and account number of the natural-person beneficiary	the contract's limitation period
2.	trading in bills of exchange	performance of contract	name, address and account number of the natural-person beneficiary	the contract's limitation period
3.	trading in cheques	performance of contract	name, address and account number of the natural-person beneficiary, cheque data	the contract's limitation period
4.	customer identification in relation to trading in foreign currency, foreign exchange (other than currency exchange services) bills of exchange and cheques on own account or as commission agents	statutory obligation (AML Act)	family name and first name, family name and first name of birth, nationality, place and date of birth, mother's birth name, address of residence, or (in the absence of such) temporary residence, type and number of identification document, politically exposed person status	8 years from the termination of the business relationship or the execution of the transaction order
5.	customer identification in relation to trading in foreign currency, foreign exchange (other than currency exchange services) bills of exchange and cheques on own account or as commission agents	statutory obligation (AML Act)	family name and first name, family name and first name of birth, nationality, place and date of birth, address of residence, or (in the absence of such) temporary residence, politically exposed person status	8 years from the termination of the business relationship or the execution of the transaction order
6.	fulfilment of the obligation to retain accounting documents	statutory obligation (Accounting Act)	data in the accounting document	8 years

A/7	Provision of sureties and bank guarantees, or the assumption of other bankers' obligations.			
1.	risk assessment prior to provision of sureties and bank guarantees, or the assumption of other bankers' obligations.	the Bank's legitimate interest	name, name at birth, place and date of birth, number and type of personal identification document, passport number, address of residence	loss of purpose/interest, or successful objection
2.	conclusion or performance of contract for provision of sureties and bank guarantees, or the assumption of other bankers' obligations	performance of the contract / consent	name, name at birth, place and date of birth, number and type of personal identification document, passport number, address of residence	contract limitation period / withdrawal of consent
3.	customer identification related to a contract for provision of sureties and bank guarantees, or the assumption of other bankers' obligations	statutory obligation (AML Act)	family name and first name, family name and first name of birth, nationality, place and date of birth, mother's birth name, address of residence, or (in the absence of such) temporary residence, type and number of identification document, politically exposed person status	8 years from the termination of the business relationship or the execution of the transaction order
4.	beneficial owner's identification related to a contract for provision of sureties and bank guarantees, or the assumption of other bankers' obligations	statutory obligation (AML Act)	family name and first name, family name and first name of birth, nationality, place and date of birth, address of residence, or (in the absence of such) temporary residence, politically exposed person status	8 years from the termination of the business relationship or the execution of the transaction order
5.	fulfilment of the obligation to retain accounting documents	statutory obligation (Accounting Act)	data in the accounting document	8 years

	Purpose of processing	Legal basis for processing	Processed personal data	Duration of data processing (erasure of data)
A) Data processing related to the provision of financial services				
A/8	Provision of safe custody service and safe deposit box service			
1.	conclusion or performance of contract for provision of safe custody services	performance of contract	name, name at birth, place and date of birth, mother's birth name, address of residence, telephone number, number and type of personal identification document, mailing address, names and positions of the natural-person authorised representatives and contacts of legal persons and entities lacking the status of a legal person.	the contract's limitation period
2.	conclusion or performance of contract for provision of safe custody services	consent	in case of application / contracting with biometric signature, the biometric data made available to the Bank with the signature on the sign pad	withdrawal of consent / contract limitation period
3.	customer identification related to contracts for provision of safe custody service	statutory obligation (AML Act)	family name and first name, family name and first name of birth, nationality, place and date of birth, mother's birth name, address of residence, or (in the absence of such) temporary residence, type and number of identification document, politically exposed person status	8 years from the termination of the business relationship or the execution of the transaction order
4.	beneficial owner's identification related to contracts for provision of safe custody service	statutory obligation (AML Act)	family name and first name, family name and first name of birth, nationality, place and date of birth, address of residence, or (in the absence of such) temporary residence, politically exposed person status	8 years from the termination of the business relationship or the execution of the transaction order
5.	conclusion or performance of contract for provision of safety deposit box services	performance of contract	name, name at birth, place and date of birth, mother's birth name, address of residence, number and type of personal identification document, mailing address, names and positions of the natural-person authorised representatives and contacts of legal persons and entities lacking the status of a legal person	the contract's limitation period
6.	conclusion or performance of contract for provision of safety deposit box services	consent	in case of application / contracting with biometric signature, the biometric data made available to the Bank with the signature on the sign pad	withdrawal of consent / contract limitation period
7.	customer identification related to contracts for provision of safety deposit box service	statutory obligation (AML Act)	family name and first name, family name and first name of birth, nationality, place and date of birth, mother's birth name, address of residence, or (in the absence of such) temporary residence, type and number of identification document, politically exposed person status	8 years from the termination of the business relationship or the execution of the transaction order
8.	beneficial owner's identification related to contracts for provision of safety deposit box service	statutory obligation (AML Act)	family name and first name, family name and first name of birth, nationality, place and date of birth, address of residence, or (in the absence of such) temporary residence, politically exposed person status	8 years from the termination of the business relationship or the execution of the transaction order
9.	fulfilment of the obligation to retain accounting documents	statutory obligation (Accounting Act)	data in the accounting document	8 years
10.	non-postal liaison	consent	e-mail address, phone number	withdrawal of consent / contract limitation period

	Purpose of processing	Legal basis for processing	Processed personal data	Duration of data processing (erasure of data)
A) Data processing related to the provision of financial services				
A/9	The issuance of paper-based cash substitute payment instruments (e.g. paper-based traveller's cheques, bills of exchange) or the provision of services related thereto that are not classified as payment services			
1.	risk management related to the issuance of paper-based cash substitute payment instruments (e.g. paper-based traveller's cheques, bills of exchange) or the provision of services related thereto that are not classified as payment services;	the Bank's legitimate interest	client's name, address, account number; natural-person beneficiary's name, address, account number; cheque data; in the case of a cheque contract, the names and positions of the natural-person authorised representatives and contacts of legal persons and entities lacking the status of a legal person	in the case of loss of purpose/interest or successful objection, or a failed contract conclusion, the time that the claim related to the failed contract conclusion becomes enforceable
2.	conclusion or performance of contract related to the issuance of paper-based cash substitute payment instruments (e.g. paper-based traveller's cheques, bills of exchange) or the provision of services related thereto that are not classified as payment services;	performance of contract	client's name, address, account number; natural-person beneficiary's name, address, account number; cheque data; in the case of a cheque contract, the names and positions of the natural-person authorised representatives and contacts of legal persons and entities lacking the status of a legal person	the contract's limitation period
3.	customer identification related to the issuance of paper-based cash substitute payment instruments (e.g. paper-based traveller's cheques, bills of exchange) or the provision of services related thereto that are not classified as payment services	statutory obligation (AML Act)	family name and first name, family name and first name of birth, nationality, place and date of birth, mother's birth name, address of residence, or (in the absence of such) temporary residence, type and number of identification document, politically exposed person status	8 years from the termination of the business relationship or the execution of the transaction order
4.	beneficial owner related to the issuance of paper-based cash substitute payment instruments (e.g. paper-based traveller's cheques, bills of exchange) or the provision of services related thereto that are not classified as payment services	statutory obligation (AML Act)	family name and first name, family name and first name of birth, nationality, place and date of birth, address of residence, or (in the absence of such) temporary residence, politically exposed person status	8 years from the termination of the business relationship or the execution of the transaction order
5.	fulfilment of the obligation to retain accounting documents	statutory obligation (Accounting Act)	data in the accounting document	8 years
6.	non-postal liaison	consent	e-mail address, phone number	withdrawal of consent / contract limitation period

	Purpose of processing	Legal basis for processing	Processed personal data	Duration of data processing (erasure of data)
A) Data processing related to the provision of financial services				
A/10	Intermediation of financial services, and intermediation of insurance under the terms provided for in the Act on Insurance Companies and the Insurance Business			
1.	intermediation of financial services	performance of contract	name, name at birth, mother's birth name, place and date of birth, nationality, address of residence, mailing address, number of personal identity card (passport), number of other identification appropriate for identifying a person under the Act on Personal Data, sex, employment, in the case of a foreign national the address of residence in Hungary; names and positions of authorised representatives of legal persons and entities lacking the status of a legal person, identification data, as specified in the foregoing, of the agent for service of process and collateral provider and other natural persons involved in the credit assessment	the contract's limitation period
2.	intermediation of financial services	consent	in case of application / contracting with biometric signature, the biometric data made available to the Bank with the signature on the sign pad	withdrawal of consent / contract limitation period
3.	intermediation of financial services	statutory obligation (Taxation Act, Personal Income Tax Act)	Tax ID number	contract limitation period / until the expiry of the right to tax determination
4.	customer identification related to the intermediation of financial services	statutory obligation (AML Act)	family name and first name, family name and first name of birth, nationality, place and date of birth, mother's birth name, address of residence, or (in the absence of such) temporary residence, type and number of identification document, politically exposed person status	8 years from the termination of the business relationship or the execution of the transaction order
5.	beneficial owner identification related to the intermediation of financial services	statutory obligation (AML Act)	family name and first name, family name and first name of birth, nationality, place and date of birth, address of residence, or (in the absence of such) temporary residence, politically exposed person status	8 years from the termination of the business relationship or the execution of the transaction order
6.	intermediation of insurance services	performance of contract	name, name at birth, mother's birth name, place and date of birth, nationality, address of residence, mailing address, number of personal identity card (passport), number of other identification appropriate for identifying a person under the Act on Personal Data, sex, employment, in the case of a foreign national the address of residence in Hungary; names and positions of authorised representatives of legal persons and entities lacking the status of a legal person, identification data, as specified in the foregoing, of the agent for service of process and collateral provider and other natural persons involved in the credit assessment	the contract's limitation period
7.	intermediation of insurance services	consent	in case of application / contracting with biometric signature, the biometric data made available to the Bank with the signature on the sign pad	withdrawal of consent / contract limitation period
8.	intermediation of insurance	statutory obligation (Taxation Act, Personal Income Tax Act)	Tax ID number	contract limitation period / until the expiry of the right to tax determination
9.	customer identification related to intermediation of insurance	statutory obligation (AML Act)	family name and first name, family name and first name of birth, nationality, place and date of birth, mother's birth name, address of residence, or (in the absence of such) temporary residence, type and number of identification document, politically exposed person status	8 years from the termination of the business relationship or the execution of the transaction order
10.	beneficial owner identification related to intermediation of insurance	statutory obligation (AML Act)	family name and first name, family name and first name of birth, nationality, place and date of birth, address of residence, or (in the absence of such) temporary residence, politically exposed person status	8 years from the termination of the business relationship or the execution of the transaction order
11.	fulfilment of the obligation to retain accounting documents	statutory obligation (Accounting Act)	data in the accounting document	8 years
12.	non-postal liaison	consent	e-mail address, phone number	withdrawal of consent / contract limitation period

	Purpose of processing	Legal basis for processing	Processed personal data	Duration of data processing (erasure of data)
A) Data processing related to the provision of financial services				
A/11	Credit pre-screening where initiated, information about credit options and contacting the inquirer about credit options and credit pre-screening using the contact details provided in the case of telephone inquiries			
1.	execution of credit pre-screening initiated by the customer	consent	name, e-mail, telephone number, year of birth, address of residence, period of residence under the same address, marital status, highest level of schooling, number of adults/children living in the same household, expenditure data, information on outstanding loan	withdrawal of consent
2.	information about credit options if requested by the customer by phone	consent	name, e-mail, telephone number, year of birth, address of residence, period of residence under the same address, marital status, highest level of schooling, number of adults/children living in the same household, expenditure data, information on outstanding loan	withdrawal of consent
3.	liaison using the contact details provided by the inquirer, regarding credit options and credit pre-screening	consent	name, e-mail, telephone number, year of birth, address of residence, period of residence under the same address, marital status, highest level of schooling, number of adults/children living in the same household, expenditure data, information on outstanding loan	withdrawal of consent

	Purpose of processing	Legal basis for processing	Processed personal data	Duration of data processing (erasure of data)
B) Provision of auxiliary financial services				
B/12	Currency exchange activity			
1.	conclusion or performance of contract for provision of auxiliary financial services	performance of contract	name, number and type of identification document, customer's legal status for currency purposes	the contract's limitation period
2.	fulfilment of the obligation to retain accounting documents	statutory obligation (Accounting Act)	data in the accounting document	8 years

	Purpose of processing	Legal basis for processing	Processed personal data	Duration of data processing (erasure of data)
C) Investment and auxiliary investment services, and other services provided by the Bank on a professional basis				
C/13	Securities lending, nominee activities, investment services, services auxiliary to investment services, and intermediation and activities available to commodity dealers under Sections 111 to 116 of the Investment Services Act.			
1.	conclusion or performance of contract for securities lending	performance of contract	name, name at birth, mother's birth name, place and date of birth, nationality, address of residence, mailing address, number of personal identity card (passport), number of other identification appropriate for identifying a person under the Act on Personal Data, in the absence of an address of residence the place of temporary residence, number of residence permit, legal status for currency purposes; names and positions of authorised representatives of legal persons and entities lacking the status of a legal person, identification data of the natural person agent for service of process	the contract's limitation period
2.	conclusion or performance of contract for securities lending	the Bank's legitimate interest	employment, name and address of employer, income status	loss of purpose/interest, or successful objection
3.	conclusion or performance of contract for securities lending	statutory obligation (Taxation Act, Personal Income Tax Act)	Tax ID number	contract limitation period / until the expiry of the right to tax determination
4.	customer identification related to contracts for securities lending	statutory obligation (AML Act)	family name and first name, family name and first name of birth, nationality, place and date of birth, mother's birth name, address of residence, or (in the absence of such) temporary residence, type and number of identification document, politically exposed person status	8 years from the termination of the business relationship or the execution of the transaction order
5.	beneficial owner identification related to contracts for securities lending	statutory obligation (AML Act)	family name and first name, family name and first name of birth, nationality, place and date of birth, address of residence, or (in the absence of such) temporary residence, politically exposed person status	8 years from the termination of the business relationship or the execution of the transaction order
6.	conclusion or performance of contract for nominee activities	performance of contract	name, name at birth, mother's birth name, place and date of birth, nationality, address of residence, mailing address, number of personal identity card (passport), number of other identification appropriate for identifying a person under the Act on Personal Data, in the absence of an address of residence the place of temporary residence, number of residence permit, legal status for currency purposes; names and positions of authorised representatives of legal persons and entities lacking the status of a legal person, identification data of the natural person agent for service of process	the contract's limitation period
7.	conclusion or performance of contract for nominee activities	the Bank's legitimate interest	employment, name and address of employer, income status	loss of purpose/interest, or successful objection
8.	conclusion or performance of contract for nominee activities	statutory obligation (Taxation Act, Personal Income Tax Act)	Tax ID number	contract limitation period / until the expiry of the right to tax determination
9.	customer identification in relation to contracts for nominee activities	statutory obligation (AML Act)	family name and first name, family name and first name of birth, nationality, place and date of birth, mother's birth name, address of residence, or (in the absence of such) temporary residence, type and number of identification document, politically exposed person status	8 years from the termination of the business relationship or the execution of the transaction order
10.	beneficial owner's identification in relation to contracts for nominee activities	statutory obligation (AML Act)	family name and first name, family name and first name of birth, nationality, place and date of birth, address of residence, or (in the absence of such) temporary residence, politically exposed person status	8 years from the termination of the business relationship or the execution of the transaction order

	Purpose of processing	Legal basis for processing	Processed personal data	Duration of data processing (erasure of data)
C) Investment and auxiliary investment services, and other services provided by the Bank on a professional basis				
C/13	Securities lending, nominee activities, investment services, services auxiliary to investment services, and intermediation and activities available to commodity dealers under Sections 111 to 116 of the Investment Services Act.			
11.	conclusion or performance of contract for provision of investment services	performance of contract	name, name at birth, mother's birth name, place and date of birth, nationality, address of residence, mailing address, number of personal identity card (passport), number of other identification appropriate for identifying a person under the Act on Personal Data, in the absence of an address of residence the place of temporary residence, number of residence permit, legal status for currency purposes; names and positions of authorised representatives of legal persons and entities lacking the status of a legal person, identification data of the natural person agent for service of process	the contract's limitation period
12.	conclusion or performance of contract for provision of investment services	the Bank's legitimate interest	employment, name and address of employer, income status	loss of purpose/interest, or successful objection
13.	conclusion or performance of contract for provision of investment services	statutory obligation (Taxation Act, Personal Income Tax Act)	Tax ID number	contract limitation period / until the expiry of the right to tax determination
14.	customer identification related to contracts for provision of investment services	statutory obligation (AML Act)	family name and first name, family name and first name of birth, nationality, place and date of birth, mother's birth name, address of residence, or (in the absence of such) temporary residence, type and number of identification document, politically exposed person status	8 years from the termination of the business relationship or the execution of the transaction order
15.	beneficial owner identification related to contracts for provision of investment services	statutory obligation (AML Act)	family name and first name, family name and first name of birth, nationality, place and date of birth, address of residence, or (in the absence of such) temporary residence, politically exposed person status	8 years from the termination of the business relationship or the execution of the transaction order
16.	conclusion or performance of contract for provision of services auxiliary to investment services	performance of contract	name, name at birth, mother's birth name, place and date of birth, nationality, address of residence, mailing address, number of personal identity card (passport), number of other identification appropriate for identifying a person under the Act on Personal Data, in the absence of an address of residence the place of temporary residence, number of residence permit, legal status for currency purposes; names and positions of authorised representatives of legal persons and entities lacking the status of a legal person, identification data of the natural person agent for service of process	the contract's limitation period
17.	conclusion or performance of contract for provision of services auxiliary to investment services	the Bank's legitimate interest	employment, name and address of employer, income status	loss of purpose/interest, or successful objection
18.	conclusion or performance of contract for provision of services auxiliary to investment services	statutory obligation (Taxation Act, Personal Income Tax Act)	Tax ID number	contract limitation period / until the expiry of the right to tax determination
19.	customer identification related to contracts for provision of services auxiliary to investment services	statutory obligation (AML Act)	family name and first name, family name and first name of birth, nationality, place and date of birth, mother's birth name, address of residence, or (in the absence of such) temporary residence, type and number of identification document, politically exposed person status	8 years from the termination of the business relationship or the execution of the transaction order
20.	beneficial owner identification related to contracts for provision of services auxiliary to investment services	statutory obligation (AML Act)	family name and first name, family name and first name of birth, nationality, place and date of birth, address of residence, or (in the absence of such) temporary residence, politically exposed person status	8 years from the termination of the business relationship or the execution of the transaction order

	Purpose of processing	Legal basis for processing	Processed personal data	Duration of data processing (erasure of data)
C) Investment and auxiliary investment services, and other services provided by the Bank on a professional basis				
C/13	Securities lending, nominee activities, investment services, services auxiliary to investment services, and intermediation and activities available to commodity dealers under Sections 111 to 116 of the Investment Services Act.			
21.	conclusion or performance of contract for provision of services provided by the intermediary of an investment firm or commodity dealer	performance of contract	name, name at birth, mother's birth name, place and date of birth, nationality, address of residence, mailing address, number of personal identity card (passport), number of other identification appropriate for identifying a person under the Act on Personal Data, income status, in the absence of an address of residence the place of temporary residence, number of residence permit, legal status for currency purposes; names and positions of authorised representatives of legal persons and entities lacking the status of a legal person, identification data of the natural person agent for service of process	the contract's limitation period
22.	conclusion or performance of contract for provision of services provided by the intermediary of an investment firm or commodity dealer	the Bank's legitimate interest	employment, name and address of employer, income status	loss of purpose/interest, or successful objection
23.	conclusion or performance of contract for provision of services provided by the intermediary of an investment firm or commodity dealer	statutory obligation (Taxation Act, Personal Income Tax Act)	Tax ID number	contract limitation period / until the expiry of the right to tax determination
24.	customer identification related to a contract for provision of services provided by the intermediary of an investment firm or commodity dealer	statutory obligation (AML Act)	family name and first name, family name and first name of birth, nationality, place and date of birth, mother's birth name, address of residence, or (in the absence of such) temporary residence, type and number of identification document, politically exposed person status	8 years from the termination of the business relationship or the execution of the transaction order
25.	beneficial owner identification related to a contract for provision of services provided by the intermediary of an investment firm or commodity dealer	statutory obligation (AML Act)	family name and first name, family name and first name of birth, nationality, place and date of birth, address of residence, or (in the absence of such) temporary residence, politically exposed person status	8 years from the termination of the business relationship or the execution of the transaction order
26.	conclusion or performance of contract for provision of services in the framework of activities available to commodity dealers	performance of contract	name, name at birth, mother's birth name, place and date of birth, nationality, address of residence, mailing address, number of personal identity card (passport), number of other identification appropriate for identifying a person under the Act on Personal Data, in the absence of an address of residence the place of temporary residence, number of residence permit, legal status for currency purposes; names and positions of authorised representatives of legal persons and entities lacking the status of a legal person, identification data of the natural person agent for service of process	the contract's limitation period
27.	conclusion or performance of contract for provision of services in the framework of activities available to commodity dealers	the Bank's legitimate interest	employment, name and address of employer, income status	loss of purpose/interest, or successful objection
28.	conclusion or performance of contract for provision of services in the framework of activities available to commodity dealers	statutory obligation (Taxation Act, Personal Income Tax Act)	Tax ID number	contract limitation period / until the expiry of the right to tax determination
29.	customer identification related to a contract for provision of services in the framework of activities available to commodity dealers	statutory obligation (AML Act)	family name and first name, family name and first name of birth, nationality, place and date of birth, mother's birth name, address of residence, or (in the absence of such) temporary residence, type and number of identification document, politically exposed person status	8 years from the termination of the business relationship or the execution of the transaction order

	Purpose of processing	Legal basis for processing	Processed personal data	Duration of data processing (erasure of data)
C) Investment and auxiliary investment services, and other services provided by the Bank on a professional basis				
C/13	Securities lending, nominee activities, investment services, services auxiliary to investment services, and intermediation and activities available to commodity dealers under Sections 111 to 116 of the Investment Services Act.			
30.	beneficiary owner's identification related to a contract for provision of services in the framework of activities available to commodity dealers	statutory obligation (AML Act)	family name and first name, family name and first name of birth, nationality, place and date of birth, address of residence, or (in the absence of such) temporary residence, politically exposed person status	8 years from the termination of the business relationship or the execution of the transaction order
31.	fulfilment of the obligation to retain accounting documents	statutory obligation (Accounting Act)	data in the accounting document	8 years
32.	non-postal liaison	consent	e-mail address, phone number	withdrawal of consent / contract limitation period

C/14	Enabling the account holder to gain information on the actual data of the securities account and the customer account on the website of the National Bank of Hungary			
1.	providing information on the actual data of the securities account and the customer account on the website of the National Bank of Hungary	statutory obligation (Investment Act)	entry identifier and password generated for securities account and customer account, securities account balance data, customer account balance data and other account data valid on the last day of the month concerned	5 years

	Purpose of processing	Legal basis for processing	Processed personal data	Duration of data processing (erasure of data)
D) Other processing cases				
D/15	Market research, opinion polls, customer satisfaction surveys			
1.	market research, opinion polls, customer satisfaction surveys	the Bank's legitimate interest	name, name at birth, mother's birth name, place and date of birth, nationality, address of residence, mailing address, number of personal identity card (passport), number of other identification appropriate for identifying a person under the Act on Personal Data, in the the case of a foreign national the address of residence in Hungary; names and positions of authorised representatives of legal persons and entities lacking the status of a legal person, identification data, as specified in the foregoing, of the agent for service of process, beneficiary's data, products and services used by the customer	loss of purpose/interest, or successful objection
2.	non-postal liaison	consent	e-mail address, phone number	withdrawal of consent / contract limitation period

D/16	Direct marketing, data controlling for marketing purposes, season's greetings, communication with individuals who use specific channels to inquire about the Bank's products			
1.	direct marketing, data controlling for marketing purposes, season's greetings, communication with individuals who use specific channels to inquire about the Bank's products	consent / the Bank's legitimate interest	name, name at birth, mother's birth name, place and date of birth, nationality, address of residence, mailing address, e-mail address, number of personal identity card (passport), number of other identification appropriate for identifying a person under the Act on Personal Data, in the the case of a foreign national the address of residence in Hungary; names and positions of authorised representatives of legal persons and entities lacking the status of a legal person, identification data, as specified in the foregoing, of the agent for service of process, beneficiary's data, products and services used by the customer In data processing for direct marketing purposes the bank performs profiling to form target groups.	withdrawal of consent, expiry of the term specified in the consent, loss of purpose/interest, or successful objection

	Purpose of processing	Legal basis for processing	Processed personal data	Duration of data processing (erasure of data)
D) Other processing cases				
D/17	Customer relations, arrangements for events, ongoing efforts to maintain data accuracy, complaints management, receivables management, other operational customer services			
1.	customer relations (liaison with the customer)	consent / the Bank's legitimate interest	name, name at birth, mother's birth name, place and date of birth, nationality, address of residence, mailing address, e-mail address, number of personal identity card (passport), number of other identification appropriate for identifying a person under the Act on Personal Data, in the the case of a foreign national the address of residence in Hungary; names and positions of authorised representatives of legal persons and entities lacking the status of a legal person, identification data, as specified in the foregoing, of the agent for service of process, beneficiary's data, products and services used by the customer	withdrawal of consent, loss of purpose/interest, or successful objection
2.	arrangements for events	consent	name, name at birth, mother's birth name, place and date of birth, nationality, address of residence, mailing address, e-mail address, number of personal identity card (passport), number of other identification appropriate for identifying a person under the Act on Personal Data, in the the case of a foreign national the address of residence in Hungary; names and positions of authorised representatives of legal persons and entities lacking the status of a legal person, identification data, as specified in the foregoing, of the agent for service of process, beneficiary's data, products and services used by the customer	withdrawal of consent
3.	continuous maintenance of data accuracy	statutory obligation (GDPR)	name, name at birth, mother's birth name, place and date of birth, nationality, address of residence, mailing address, e-mail address, number of personal identity card (passport), number of other identification appropriate for identifying a person under the Act on Personal Data, in the the case of a foreign national the address of residence in Hungary; names and positions of authorised representatives of legal persons and entities lacking the status of a legal person, identification data, as specified in the foregoing, of the agent for service of process, beneficiary's data, products and services used by the customer	contract limitation period / withdrawal of consent, loss of purpose/ interest, or successful objection / term determined by law
4.	complaint management (except for recording phone conversations related to the complaint)	statutory obligation (Credit Institutions Act)	name, name at birth, mother's birth name, place and date of birth, nationality, address of residence, mailing address, e-mail address, number of personal identity card (passport), number of other identification appropriate for identifying a person under the Act on Personal Data, in the the case of a foreign national the address of residence in Hungary; names and positions of authorised representatives of legal persons and entities lacking the status of a legal person, identification data, as specified in the foregoing, of the agent for service of process, beneficiary's data, products and services used by the customer	5 years
5.	management of receivables related to the concluded contract (collection of receivables)	consent / the Bank's legitimate interest	name, name at birth, mother's birth name, place and date of birth, nationality, address of residence, mailing address, number of personal identity card (passport), number of other identification appropriate for identifying a person under the Act on Personal Data, in the the case of a foreign national the address of residence in Hungary; names and positions of authorised representatives of legal persons and entities lacking the status of a legal person, identification data, as specified in the foregoing, of the agent for service of process, beneficiary's data, products and services used by the customer	loss of purpose/interest / successful objection, or withdrawal of consent
6.	non-postal liaison conducted for receivables-collection purposes (except for telephone conversations)	consent	telephone number, e-mail address	loss of purpose or withdrawal of consent
7.	fulfilment of the Bank's quality assurance objectives	consent	name, name at birth, mother's birth name, place and date of birth, nationality, address of residence, mailing address, number of personal identity card (passport), number of other identification appropriate for identifying a person under the Act on Personal Data, in the the case of a foreign national the address of residence in Hungary; names and positions of authorised representatives of legal persons and entities lacking the status of a legal person, identification data, as specified in the foregoing, of the agent for service of process, beneficiary's data, products and services used by the customer	loss of purpose or withdrawal of consent
8.	verifying the authenticity and appropriateness of the personal data provided, and, in line with Recommendation 14/2012. (XII.13.) of PSZÁF (Hungarian Financial Supervisory Authority), retrieving new address data through GRIInfO for establishing the liaison required in order to facilitate the debtor's performance or to avoid legal proceedings, or, if all this fails, to initiate a recovery process by means of legal proceedings	consent, the Bank's legitimate interest	name, address of residence, mailing address	withdrawal of consent / contract limitation period

	Purpose of processing	Legal basis for processing	Processed personal data	Duration of data processing (erasure of data)
D) Other processing cases				
D/18	Performance of the Agreement between the Government of Hungary and the Government of the United States of America to Improve International Tax Compliance and to Implement the FATCA			
1.	fulfilment of obligations under the FATCA	statutory obligation (FATCA Act)	name, address, United States tax ID number, account number, account balance	5 years

D/19	Audio-recordings produced in the Bank's call center and other similar customer service / relevant sales areas operating on similar principles			
1.	audio-recording of phone conversation conducted in the context of complaint management	statutory obligation (Credit Institutions Act)	time of audio-recording, time of call, caller's telephone number, minutes of audio-recording	5 years
2.	execution of an order submitted to the Bank, if the object of the telephone conversation is a specific order	performance of contract	time of audio-recording, time of call, caller's telephone number, transcript of the audio-recording, if any	8 years
3.	ensuring traceability of telephone conversations (including those regarding collection of receivables) conducted with the customer (excluding complaints or specific orders), and fulfilment of the Bank's quality assurance objectives	consent	audio-recording, time of call, caller's telephone number, transcript minutes of the audio-recording, if any	loss of purpose or withdrawal of consent, but not more than 8 years

D/20	Monitoring, for property protection and security purposes, of entry to and exit from specific buildings and premises used by the Bank			
1.	personal, property, data security / protection	the Bank's legitimate interest	name, number of personal identification document, fact and time of passing checkpoints	in the the case of regular entry until termination of the entry authorisation, but not more than 6 months from the time of generation of the data in the case of casual entry, for 24 hours from departure / successful objection

	Purpose of processing	Legal basis for processing	Processed personal data	Duration of data processing (erasure of data)
D) Other processing cases				
D/21	Production and retention of video recordings made, for the protection of confidential securities and business information, security, and the protection of human life and physical integrity, of natural persons intending to enter, for specific purposes, to the Bank's seat and establishments and other buildings used by the Bank as private areas open to the public			
1.	protection of private but publicly used areas that are required for the fulfilment of the Bank's duties; personal, property and data security, protection	the Bank's legitimate interest	video-recording	60 days / successful objection

D/22	Data controlling regarding to consumer clients of UniCredit Leasing Hungary Zrt.			
1.	liaising with the clients of UniCredit Leasing Hungary Zrt. to make preliminary credit assessment and tailor-made loan offers	the Bank's legitimate interest	name, date and place of birth, mother's name, date of decision, net monthly income (HUF), monthly instalment of outstanding debt (HUF), new demand obligation, monthly household expenditure, education, profession, number of persons living in the household, number of dependents, employer's tax number / company registration number / KSH number, address, address type, current UniCredit Leasing delay (days, amount), maximum number of delayed days in the last 6/12 months, maximum overdue debt in the last 6/12 months, sold/written claim in the past 5 years, initial date of employment, sector of employment, date of occupation	loss of purpose/interest, or successful objection, but not more than 60 days of delivery of the data
2.	liaising with the clients of UniCredit Leasing Hungary Zrt. to make preliminary credit assessment and tailor-made loan offers	consent	telephone number, e-mail address	withdrawal of consent

III. Data Transfer

The bank has the right to transfer data in relation to processing, based on the data subject's consent or under a statutory provision (recipients are other potential controllers outside the Bank), as follows:

Based on the data subject's voluntary consent:

- in the case of document verification and other retrieval, to the Central Office for Administrative and Electronic Public Services (1094 Budapest, Balázs Béla u. 35)
- in the case of income verification by the National Tax and Customs Administration (1054 Budapest, Széchenyi u. 2, www.nav.gov.hu) or by the employer
- to the Bank's Intermediary, in the reconciliation regarding the intermediation fee

Based on Articles 161-164 of the Credit Institutions Act on the release of bank secret and Articles 118-120 of the Investment Services Act on the release of securities secret:

- to the Bank's owner, UniCredit S.p.A. (20154 Milan, Italy, Piazza Gae Aulenti 3 – Tower A, www.unicreditgroup.eu), for purposes related to ownership control, to the fulfilment of the Bank's statutory tasks and obligations, to consolidation, risk analysis and sales of services, and to ensure compliance with requirements related to the consolidated supervision
- to UniCredit Bank Austria AG, as per Sections 8 and 9 of Annex 1 of the General Business Conditions on outsourced activities (hereinafter: Outsourcing Annex)
- to third parties, receivables managers engaged on receivables collection activities, in order to enforce the Bank's claims

Based on Article 5 (2) of the CCIS Act:

- to BISZ Zrt., when retrieving reference data from the CCIS or in the case of data transfer

Based on Article 142/A (2)-(3) of the Capital Market Act.

- to the National Bank of Hungary, in relation to the processing referred to in section I/C/14.

IV. Data processors

- in the case of retrieval from GIRinfo, to GIRO Zrt. (1054 Budapest, Vadász u. 31., info@mail.giro.hu, www.giro.hu)
- to the Bank's business partners contracted for purposes related to opinion polls, market research and direct marketing

- in the case of processing performed for property protection and security purposes (section I/D/D/21-22), Honeywell Szabályozástechnikai Kft. (1139 Budapest, Petneházy u 2-4. 3. em.), CRITERION Biztonsági Szolgáltatások Zrt. (1033 Budapest, Polgár u 8-10.)

Data processors and sub-data processors in the course of outsourcing under Section 68 of the Credit Institutions Act:

- EPDB Nyomtatási Központ Zrt. (seat: 1117 Budapest, Budafoki út. 107-109.) 1117 Budapest, Budafoki út. 107-109.) as data processor and sub-data processor Díjbeszedő Informatikai Kft. (1117 Budapest, Budafoki út 107-109.) according to Sections 1 and 4 of the Outsourcing Annex
- Iron Mountain Kft. (seat: 1093 Budapest, Czuczor utca 10.) as data processor and Datashred Kft. (1012 Budapest, Kuny Domokos utca 4/D fsz.1.) as sub-data processor according to Sections 2 and 9 of the Outsourcing Annex
- THALES DIS Deutschland GmbH (Warinherstrasse 81, 81541 München, Germany) as data processor and ANY Biztonsági Nyomda Nyrt. (1102 Budapest, Halom u. 5.) as sub-data processor according to Section 3 of the Outsourcing Annex
- UniCredit Services S.C.p.A ("US") (Italy, 20151 Milan, Via Livio Cambi 1.) as data processor and sub-data processors under https://www.unicreditbank.hu/content/dam/cee2020-pws-hu/Rolunk/US_ScPA_al-adatfeldolgozok-Sub-data-processors.pdf according to Section 5 of the Outsourcing Annex
- UniCredit Bank AG. (Kardinal-Faulhaber- Str. 1, 80333 Munich, Germany) according to Section 6 of the Outsourcing Annex
- NeoSoft Informatikai Szolgáltató Kft. (8000 Székesfehérvár, Távírdá utca 2/A.) according to Section 10 of the Outsourcing Annex
- UniCredit Business Integrated Solutions Austria GmbH (1090 Vienna, Nordbergstrasse 13) as data processor and B.I.T. Blue IT-Services Ges.m.b.H. (AT 1020 Vienna Obere Donaustraße 95), COMARCH SPOLKA AKCYJNA (PL 31-864 Krakow Aleja Jana Pawla II 39a), EXPERIAN ÖSTERREICH GESELLSCHAFT MI (AT 1080 Wien Strozsigasse 10), PL-O-T EDV-Planungs- und Handels GmbH (AT 1010 Wien Franz Josefs Kai 33), SPECIFIC-GROUP SLOVAKIA KG (SK 821 04 Bratislava Galvaniho 7/D), Targit GmbH (AT 1040 Vienna Brucknerstraße 2/3), TERADATA GMBH (AT 1150 Wien Storchengasse 1), VOQUZ IT Solutions (AT 1030 Wien Rennweg 97-99) as sub-data processors according to Section 11 of the Outsourcing Annex

- GIRO Elszámolásforgalmi Zártkörűen Működő Részvénytársaság (1054 Budapest, Vadász u. 31.) according to Section 12 of the Outsourcing Annex
- Afford Fordító- és Tolmácsiroda Kft. (1093 Budapest, Lónyay utca 29.) as data processor and Syntext Bt. (1147 Budapest, Czobor u. 84/B), Horváth Eleonóra ev. (8000 Székesfehérvár, Havranek u. 6.), Punktum 03 Bt. (1133 Budapest, Kárpát u. 5.), Mezei Viola Mezei ev. (1021 Budapest, Budakeszi út 55/D) és Világ-Egyetem Kft. (1064 Budapest, Vörösmarty u. 42. 2/16.) as sub-data processors according to Section 13 of the Outsourcing Annex
- InterContact Budapest Kft. (1054 Budapest, Hold u. 15.) as data processor és SB Bt. (1122 Bp., Maros u. 25.), Csere Éva és Tsa Bt. (1028 Budapest, Úrbéres u. 38-40.), Exedrium Kft. (1016 Budapest, Fenyő u. 13.), Konsulinna Bt. (1016 Budapest, Fenyő u. 13.), Target 27. Kft. (2600 Vác, Karcsu Antal Arzén u. 1/C.), B.O. Bt. (1101 Budapest, Kőbányai út 43/A, Aldwick Kft. (5600 Békéscsaba, Andrássy u. 24-28.), Krahobor Bt. (2086 Tinnye, Honfoglalás u. 7.), Márk Frivaldszky e.v. (1046 Budapest, Kunhalom. u. 28.), Szomráky Béla e.v. (2626 Nagymaros, Béla Király u.2.), Al-Dente Bt. (1138 Budapest, Népfürdő u. 17/C.), Bezdán Csaba e.v. (7622 Szedeg, Attila út 7.), Mahalo Bt. (1031 Budapest, Vízimolnár u. 6.), Trans-Script Bt. (1032 Kiscelli u. 18.), Kaletsky és Tsa Kft. (1012 Budapest, Logodi u. 50.), a RG Progress Bt. (1145 Budapest, Róna u. 185.), Niles Facklam e.v. (77694 Kehl, Kindergarten Strasse 1/A.) és Szunyiné Vezse Mária e.v. (2030 Érd, Bibic u. 46.) as sub-data processors according to Section 14 of the Outsourcing Annex
- Interlingo Bt. (1026 Budapest, Pasaréti út 47.) according to Section 15 of the Outsourcing Annex
- Criterion Készpénzlogisztikai Korlátolt Felelősségű Társaság (1139 Budapest, Rozsnyai u. 21-25.) according to Section 16 of the Outsourcing Annex.
- e-Jogsegéd Szolgáltató Korlátolt Felelősségű Társaság (1135 Budapest, Kisgömb utca 6/1.) according to Section 17 of the Outsourcing Annex.
- Interlex Communications Kft. (1013 Budapest, Attila út 33.) according to Section 18 of the Outsourcing Annex.
- BSCE Tanácsadó és Informatikai Kft. (Magyarország, 1134 Budapest, Róbert Károly körút 82-84.) according to Section 19 of the Outsourcing Annex.
- Ingenico Hungary Kft. (1134 Budapest, Váci út 19.) according to Section 20 of the Outsourcing Annex.
- SIA Slovakia a.s. (Einsteinova 25, 851 01 Bratislava, Slovakia) and SIA Central Europe a.s. Magyarországi Fióktelepe, (1117 Budapest, Alíz utca 4.) according to Section 21 of the Outsourcing Annex.
- MaritzCx GmbH (22765 Hamburg, Borselstrasse 18., Germany) according to Section 22 of the Outsourcing Annex.

