General Terms and Conditions for the provision of Internet Banking System services by ING Bank Śląski S.A. for holders of the Refugee Account

effective from 22 March 2026

Table of contents

1. General Provisions

Article 1

1. The ING Bank Śląski S.A. Internet Banking System for holders of the Refuge Account is the trade name of the electronic banking service referred to in the Regulation of the Minister of Development and Finance on the list of representative services linked to a payment account of 14 July 2017 (hereinafter: Regulation). According to the Regulation, the electronic banking service provides access to a payment account via the Internet, allowing users to check the balance of the payment account, change limits for cashless payments and debit card transactions or to submit other types of instructions to the account. The Internet banking system of ING Bank Śląski S.A. for holders of the Refugee Account may also include services unrelated to payment accounts. In these General Terms and Conditions, the trade names (i.e. Internet Banking System, System) will be used to refer to the electronic banking service.
2. The terms and abbreviations used in these General Terms and Conditions mean:
   1) **address for electronic delivery** – the electronic address of an entity using the public registered electronic delivery service or the public hybrid service or the qualified registered electronic delivery service, as described in the Act of 18 November 2020 on electronic delivery, enabling the unambiguous identification of the sender or recipient of the data sent as part of those services. This address will be made available on the Bank's website;
   2) **mobile application** – the Bank's application for mobile devices. It is part of the Internet Banking System and can also be accessed by installing it on the user's mobile device. The mobile application may be available in different versions and under different brand names among others: "Moje ING application" or "Moje ING mobile" or other names. The list of mobile applications designed for a specific type of mobile devices, technical requirements, scope of functionality, including the types of instructions that can be submitted using them, is described in the Announcement:
   3) **Bank** – ING Bank Śląski Spółka Akcyjna with its registered office in Katowice, ul. Sokolska 34, 40-086 Katowice, entered into the Register of Entrepreneurs of the District Court Katowice-Wschód, 8th Commercial Division of the National Court Register under the number KRS 0000005459, with a share capital of PLN 130,100,000 and paid-in capital of PLN 130,100,000, NIP 634-013-54-75, with an international SWIFT identification code (BIC) – INGBPLPW and e-mail address info@ing.pl, supervised by the Polish Financial Supervision Authority with its registered office in Warsaw, ul. Piękna 20, 00-549 Warsaw, conducting, on the basis of authorisations of the Polish Financial Supervision Authority, brokerage business via the organisationally separate Brokerage Office of ING Bank Śląski S.A (Biuro Maklerskie ING Banku Śląskiego S.A.);
   4) **biometric reader** – a functionality of a mobile device provided by its manufacturer or a manufacturer of the software installed on it. It is used to read biometric characteristics and store them in the device to create a corresponding digital user key;
   5) **instruction** – any statement made by the user, a payment order is also an instruction;
   6) **business day** – a day other than a Saturday or a public holiday;
   7) **password** – a string of characters set by the user. It is used to log in to the Internet Banking System and to assign a PIN code to the mobile application. The number and type of characters of a password are indicated by the system at the time it is set;
   8) **biometric identifier – a user key created on the mobile device and digitally stored in it, generated for one specific biometric ch**aracteristic of the user and corresponding to a unique code created by the Bank. For example, such a biometric characteristic could include a fingerprint or individual facial features. The unique code is permanently linked to the user's login. This code is created when the user accepts the authentication method or authorises the instruction with the biometric identifier. The user may withdraw consent to his/her authentication or authorisation of instructions using a biometric identifier by disabling this method in the mobile application. The relevant biometric characteristic and the aforementioned user key must not be communicated to or stored by the Bank;
   9) **user identifier (also called login)** – an individual string of characters assigned to a user by the Bank, used for logging into the Internet Banking System, including the mobile application. It consists of six letters and four random digits and may also be required to authenticate the user;

10) **helpline** – a telephone line intended for providing information, servicing selected bank products and services, as well as services or products of entities, which are offered by the Bank or are related to the Bank's operations. The list of activities carried out on the helpline is made available on the notice board in bank outlets and on the Bank's website;
11) **one-time activation code** – a sequence of letters and numbers generated randomly by the Bank. It is used to assign a password to the Internet Banking System and to establish a telephone number for authorisation;
12) **security key** – a device conforming to the standard described in the Announcement, connected to a computer or mobile device, used in the authentication or authorisation process in the Online Banking System. Authentication and authorisation using this security key is possible when the Bank provides this functionality;
13) **authorisation code, code for authorisation (code)** – a sequence of digits or letters or other characters, which is used to authenticate the user, including during the activation of the System or the mobile application, or for one-off authorisation of instructions submitted by the user, including payment instructions. This code may also be required to access the System, including the mobile application or device, or to submit an instruction. This code is generated by the Bank unless the type of code is set by the user. The type of authorisation code can be, for example, a text message code, a PIN code, a code transmitted by voice during an
automated telephone call. Whenever the General Terms and Conditions allow authentication or authorisation by means of a biometric identifier and you have enabled the method of authentication or authorisation by means of a biometric identifier, it is an authorisation code for the purposes of the General Terms and Conditions;
14) **PIN code** – a multi-digit code for logging into the mobile application, authorisation of instructions or payment orders. It is set and changed by the user. At the time of setting or changing it, the Bank informs the user of the required number of digits making up the PIN code;
15) **Announcement** – a message issued by the Bank to the users of the Internet Banking System for holders of the Refugee Account;
16) **Convention** – Convention of 5 October 1961 abolishing the requirement of legalisation for foreign public documents;
17) **security key list** – contains all the keys that the user considers secure and that meet the technical requirements set out in the Announcement. The user can modify the list of the activated keys by adding or removing individual keys from the list. The list may contain one or more keys;
18) **list of trusted browsers (hereinafter: the list of browsers)** – contains all the browsers which the user considers secure and which meet the technical requirements set out in the Announcement and with which the user chooses to use online banking. The user can modify the list of browsers by adding or removing individual browsers from the list. The list of browsers can contain one or more browsers (maximum 5). The browser is listed at the time of logging in to online banking via a web browser. The Bank may require the provision or confirmation of data or information to confirm the user's identity before listing a particular web browser as a trusted browser. This may also include such information which, to the Bank's knowledge, is known only to the user. Such a web browser is hereinafter referred to as a trusted browser;
19) **list of trusted mobile devices (hereinafter: the list)** – contains all the mobile devices which the user considers secure and which comply with the security rules set out in the General Terms and Conditions and with which the user decides to use the mobile application. The list may contain one or more devices. A mobile device is added to the list when the mobile application is activated on it. Before enrolling a device as a trusted mobile device, the Bank may require the provision or confirmation of data or information to identify the user's identity. This may also include such information which, to the Bank's knowledge, is known only to the user. Such a device is hereinafter referred to as a trusted mobile device;
20) **NFC** (Near Field Communication) is a short-range, high-frequency, radio communication standard that allows wireless data exchange over a distance of up to 20 centimetres;
21) **payee** – a natural person, a legal person and an organisational unit without legal personality to which the law grants legal capacity, being the recipient of funds transferred as part of a payment transaction;
22) **branch** – a group of units or outlets dealing with direct client service or operational service at the Bank;
23) **protection period** – a period during which we may not accept your order for security reasons. The protection

period may be activated after enabling certain functions in the System that require additional security checks, e.g. after a significant increase in transaction limits or after activating sensitive transfers. The protection period may last up to 6 hours. We will inform you about the activation of the protection period in Moje ING;

24) **bank outlet** – a place where the client is served by a specialist or an employee of a Bank's partner. A bank outlet includes a meeting place, a cash point, a point of sale. Bank outlets are either located in a branch or outside a branch. Information on the scope of service at a given bank outlet is available in the List of activities performed at bank outlets and via the Bank's helpline. The list is available on notice boards at the bank outlets and on the Bank's website;

25) **payer** – a natural person, a legal person and an organisational unit without legal personality to which the law grants legal capacity, who submits a payment order;

26) **PUSH/push notification** – a type of message that is displayed on a trusted mobile device on which the mobile application has been installed. In order to receive push messages, the user must have this function enabled on the mobile device on which the mobile application is installed and must agree to receive them. The operating systems for which the Bank provides pushes are specified in the Announcement;

27) **sensitive transfers** – payments that require activation by you in Moje ING. For security reasons, they may be subject to a protection period after activation. Sensitive transfers include foreign currency transfers and express transfers. We may disable the sensitive transfer feature if you do not use it for a period of 90 days;

28) **acceptance button** – a button used by the user to confirm the submission of an instruction. It may be marked with logos or names, e.g. "Send", "Approve", "Confirm", "Order", "Accept". Depending on the instruction, it may be posted at different locations in the Online Banking System;

29) **point of sale** – a bank outlet where the client is served by an employee of a Bank partner. Banking activities or factual activities that are related to banking activities for the Bank are performed at the point of sale by the Bank's partner or its employees;

30) **payment account** – means a payment account within the meaning of the Payment Services Act. The contractual regulations binding the client which apply to the account in question must contain information on whether the type of account held with the Bank is a payment account;

31) **savings account** – a payment account as defined in the Terms and Conditions of Accounts for Individual Clients;

32) **savings and settlement account** – a payment account within the meaning of the General Terms and Conditions for holders of the Refugee Account;

33) **General Terms and Conditions** – these General Terms and Conditions;

34) **General Terms and Conditions for Accounts for Individual Clients** – General Terms and Conditions for the provision of services by ING Bank Śląski S.A. as part of maintaining the Account for Refugees;

35) **strong user authentication (referred to as strong authentication)** means an authentication procedure which we apply in accordance with the law and which ensures the protection of the confidentiality of data and requires the confirmation of at least two of the elements belonging to different categories: the exclusive knowledge of the user, the exclusive possession by the user of a specific thing or a characteristic of the user. This confirmation must be independent in such a way that a breach of one of its elements does not undermine the credibility of the others. Confirmation of these circumstances will require the user to provide elements such as, for example:

   a) passwords, or

   b) a payment card in any form, including card details such as the card number, expiry date, or

   c) an identification or authorisation code, or

   d) biometric characteristics, including those provided to devices with a fingerprint reader, such as a telephone or any other device with a fingerprint reader or facial biometric reader,

   e) use of security keys,
   or other information indicating that the user is in the possession of a specific item, appliance or characteristic. This element will also be deemed to have been satisfied if the user's device is considered verified. Verification can be done by the Bank remotely determining the hardware or software characteristics of the device. Verified devices are, for example, a trusted mobile device, other devices or things on which a payment card issued by the Bank is installed;

36) **force majeure** – an external event, beyond the Bank's control, which the Bank could not prevent or foresee and which directly or indirectly led to non-performance or improper performance of the agreement by the Bank. The following events meeting the above conditions are considered force majeure:

   a) flood, earthquake, lightning, hurricane, tornado, volcanic eruption, or other similar atmospheric phenomena,

   b) power cut by the electricity provider for reasons beyond the Bank's control.

   The force majeure provisions will also apply in the event of an act of government (such as an international agreement, law, regulation, order, resolution issued by a competent authority/administration), pursuant to which a certain transaction or transactions of a certain type or with certain entities or transactions at a certain time may not be made by the Bank. The Bank will make public the fact that force majeure has occurred and, if possible, advise the expected duration of the force majeure;

37) **Internet Banking System, Internet Banking, System** – trade names which, when used in the Agreement, General Terms and Conditions and Announcement, mean the electronic banking service for holders of the Refuge Account. The internet banking system for holders of the Refuge Account is for its users only and is accessible via a device with a web browser and internet connection or a mobile application. It may come in different versions which may have different trade names e.g.: "Moje ING" or other. Different named versions of the System may differ in their technical requirements;

38) **authorisation telephone** – the User's mobile telephone number intended for receiving authorisation codes or performing services covered by the Agreement or the General Terms and Conditions. This telephone may also be used to receive information or notifications from the Bank. These may relate, among other things, to the security of transactions or changes to the General Terms and Conditions or other contractual terms. The authorisation phone number is indicated by the user when applying for access to the System or entering into an Agreement or assigning a password to the System. The user may change the telephone number for authorisation in the manner specified by the Bank;

39) **payment transaction/transaction** – a deposit, transfer or withdrawal of funds initiated by the payer or the payee, which changes the balance of funds on the account;

40) **contactless transaction** – a type of transaction that is executed using contactless technology at a merchant's terminal (Point of Sale terminal) or ATM equipped with a contactless reader;

41) **restricted access mode to Moje ING** – a mode that you can activate yourself in the System by enabling the function of restricting access to Moje ING. Activating this mode means that you cannot submit instructions in the System. You will still be able to view your data and contact the bank.
   You can deactivate the limited access mode in Moje ING after the protection period indicated by us during activation or earlier at a bank branch;

42) **Agreement** – an agreement concluded between the user and the Bank – which is the Agreement for the use of electronic banking systems for holders of the Refugee Account, the subject matter of which is the provision of the Internet Banking System service. Such an agreement is the Agreement for the use of electronic banking systems for holders of the Refugee Account.
   Whenever other documents, including agreements or annexes refer to an Agreement for the use of electronic banking systems for holders of the Refugee Account, it should be taken to mean the Agreement;

43) **unique identifier** – a combination of letters, numbers or symbols specified by the Bank, which is provided by the payer/payee in order to unambiguously identify the other payer/payee involved in the payment transaction or his/her account. The General Terms and Conditions describe a unique identifier for each type of transaction. Unless otherwise set out in the Agreement or the General Terms and Conditions, the unique identifier is the payee's bank account number or mobile phone number. For the mobile telephone number of the payee or of a person authorised to act on his/her behalf to be a unique identifier, it must first be linked to a single account number of the payee or linked to the payee in such a way that the payee can be unambiguously identified. The principles of establishing this link are described in the General Terms and Conditions;

44) **act on payment services, Act** – the Act of 19 August 2011 on payment services;

45) **mobile device** – a multifunctional portable device with Internet access that integrates the functions of a computer or mobile phone. The list of operating systems for mobile devices intended for use with the mobile application is indicated in Art. 28 sec. 3 of the General Terms and Conditions, in the Announcement and on

the Bank's website;

46) **authentication** – a procedure that allows the Bank to verify a user's identity or the validity of the use of a given payment instrument, including his/her individual credentials. The General Terms and Conditions specify what data or information is to be provided to verify identity;

47) **user** – a person who is a party to the Agreement;

48) **List** – a list of activities performed at outlets and via the Bank's helpline, containing information on the scope of services performed at a given bank outlet. The list is made available on notice boards at the bank outlets and on the Bank's website for information purposes.

49) **payment order** – a declaration of intent by the payer or payee addressed to the Bank, containing an instruction to execute a payment transaction.

3. Whenever the Account Agreement refers to a branch/outlet of the Bank in respect of an activity, it should be taken to mean the bank outlet where the activity is performed. Information on which bank outlets perform which activity can be found in the List. The list is available on notice boards at the bank outlets and on the Bank's website.
4. Whenever the General Terms and Conditions refer to a bank outlet in respect of an activity, the information on which bank outlet performs which activity can be found in the List. The list is available on notice boards at the bank outlets and on the Bank's website.
5. We will make information on how we meet accessibility requirements available on our website www.ing.pl. [Legal basis: Act on ensuring that economic operators meet the accessibility requirements for certain products and services]

Article 2

1. The General Terms and Conditions set out the terms and conditions under which the Bank provides the services of the Internet Banking System to holders of the Refuge Account.
2. The subject of the provision of services are the Internet Banking System services described in the General Terms and Conditions that enable the Bank to provide financial services through this System.
3. The System allows the user to access only those services, including accounts, to which he/she has been authorised. An authorised person will be understood as a person authorised to give a specific instruction in accordance with a separate agreement.
4. Where specific financial services available in the system are subject to risks due to their specific features or the nature of the activity or the remuneration dependent on price movements in the financial market, those risks will be described in the agreements or regulations (general conditions of agreements) governing the service in question. Risks related to the services of the Internet Banking System may consist in a breach of the security rules described in the General Terms and Conditions, in particular those described in the general terms and conditions for the secure use of the System in Chapter 16, or in the risk of making devices or applications available to unauthorised persons.
5. The internet banking system is available 24 hours a day, 7 days a week. The relevant time for execution of payment orders and other instructions through the System is Central European Time (CET) or Central European Summer Time during the period of its adoption until cancelled.
6. A proposal to conclude the Agreement which includes the Terms and Conditions, will not be binding unless its binding character is expressly provided for in the Bank's proposal.
7. There is a Bank Guarantee Fund, which operates on the principles set out in the Act on this Fund. The information sheet for that Fund will be provided by the Bank to the account holder pursuant to a separate account agreement. The sending of the fact sheet and the confirmation of its receipt by the user who is the account holder may be done via the System.
8. The language used in the Bank's relations with its clients, also when the Bank acts on behalf of another entity as an intermediary, agent or representative, is Polish.
9. The law governing the Bank's relationship with the account holder prior to the conclusion of the agreement and the law applicable to the conclusion and performance of the agreement is the Polish law (law of the Republic of Poland).
10. If a user who is a party to the Agreement is also a party to an agreement for a specific bank account or a party to other agreements concluded with or through the Bank, and access to those accounts, services or products is

provided via the Internet Banking System, any matters not governed by the General Terms and Conditions will be governed by the provisions of the agreements concluded by the client, including general terms and conditions.

11. The user through the System can, as far as it is allowed by law, make: identification and authentication in the electronic platform of public administration services, authorisations connected with the use of a trusted profile and confirmation of a trusted profile.

12. Whenever General Terms and Conditions for the provision of Internet Banking System services by ING Bank Śląski S.A. are referenced in other regulations applicable to the Bank's products and services, they are to be taken to mean these General Terms and Conditions.

13. The Announcement is not an integral part of the Terms and Conditions and is for information purposes only. A change of the content of the Announcement does not result in an amendment to the General Terms and Conditions and does not require the General Terms and Conditions to be terminated.

14. The Bank provides the full text of the Announcement:

1) at bank outlets – on notice boards,

2) on the Bank's website.

15. A change of the content of the List will not result in an amendment to the General Terms and Conditions and will not require the List to be terminated. The current content of the List is made available on notice boards at bank outlets and on the Bank's website.

2. Conclusion of the Agreement

Article 3

1. The agreement is concluded for a specified period of time.

2. The agreement may be concluded at a bank outlet providing this service, provided, however, that the Bank has the right to exclude the possibility of concluding agreements at indicated bank outlets,

3. The agreement may be concluded by a client who is a natural person with full legal capacity,

4. The Bank does not make the Internet Banking System available to partially or completely legally incapacitated persons.

5. Where required by law, the Bank, prior to making some of the functionalities/services indicated in the Announcement available to the user, verifies the user's identity on the basis of an identity document submitted by the user during his/her personal appearance at a bank outlet. This provision will not apply where such verification has been made as part of the process of concluding the Agreement.

3. Access to the system

Article 4

1. At the time of applying for access to the System or, at the latest, after concluding the Agreement, the Bank provides each user with a login and a one-time activation code or authorisation code.

2. In order to use the Internet Banking System, the user must first activate it. Activation of the System means assigning a self-defined password with the use of which the user will log on to the System.

3. In order to assign a password to the System, an authorisation code is required, which is delivered in a text message sent by the Bank to the telephone number provided by the user for authorisation or a one-time activation code delivered at the bank branch carrying out this activity or by mail to the correspondence address provided by the user. The authorisation code and the one-time activation code may be provided in another form agreed between the Bank and the user.

4. The validity period of the authorisation code may be limited for System security reasons. The standard validity period is limited to the duration of the session, i.e. the time of the user's connection with the Bank. A one-time activation code is valid for 30 days from the date the user ordered it.

5. If the user has received a one-time activation code by post, they must call the helpline to confirm its delivery. If the user does not confirm the delivery of the one-time activation code by telephone, he/she will not be able to assign a password and use the System.

6. If the mail with the one-time activation code is damaged or if the one-time activation code is illegible, the user should file a claim immediately.

Article 5

1. The Bank will notify the user how the login will be provided when concluding the Agreement or when applying for access to the Internet Banking System.

Article 6

1. In order to assign a password to the System, the user is required to complete the relevant application form which can be found on the Bank's website. The user may also be asked to set a password for the System when applying for access to the Internet Banking System.
2. For reasons of IT security of the System or security of the deposited funds, the Bank may make the submission of applications conditional upon the user providing certain personal data or information relating to the service in question.
3. If the user has not used the one-time activation code/authorisation code within its validity period, the user should request that the Bank provides him/her with a new code.

4. User authentication

Article 7

1. The user logs into the Internet Banking System personally, using only his/her own data which authenticate him/her (e.g. the login which the Bank has assigned to him).
2. User authentication is required both when logging into the System and when initiating an electronic payment instruction. Subject to sec. 3, 4 and 5, the authentication of the user when logging on to the Internet Banking System includes the following actions:
   1) providing a valid login,
   2) providing a masked password, which means that the user enters password characters selected randomly by the System,
   3) and, where required by law or for security reasons, also the relevant authorisation code or confirmation in the mobile application, if the user has the mobile application, or the use of the security key, if the user has an active key on the list of security keys.

   If, when the user logs into the System, the Bank requires all the information referred to in 1) – 3) above to be provided, this is called strong authentication. The Bank uses strong authentication when required by law.
3. Authenticating a user when logging into a mobile application requires the following steps on a trusted mobile device:
   1) providing a valid login – the first time you log in,
   2) providing a masked password at first login and a PIN code at subsequent logins,
   3) providing a masked password at first login and a PIN code at subsequent logins, where the mobile application is installed on a mobile device equipped with a biometric reader, subsequent logins may be performed by means of:
      a) a biometric identifier, if the user has chosen this method of authentication,
      b) and, where required by law or for security reasons, additionally appropriate authorisation code which is not a biometric identifier (e.g. a text message code or a PIN code) may also be required.

   4) where required by law or for security reasons, additionally the use of a security key when the user has an active key in the list of security keys.

   Authentication is called strong authentication if, when logging into the mobile application, the Bank requires the possession of a trusted mobile device and, moreover, the provision of all information referred to in p. 1) and 2) or information referred to in p. 3). In order to prevent unauthorised logins, the Bank has the right to introduce additional means or ways of authenticating the user when logging in to the System. The Bank may introduce additional means of authentication, including where required by law.

4. User authentication with a security key requires the user:
   1) to register the security key in the online banking system,
   2) to activate the security key at a bank branch or the bank's call centre, or through the internet banking system, if the bank offers such a possibility, and to agree to such an authentication method.
5. Subject to sec. 7, in order to select an authentication method using a biometric identifier, the user should first:
   1) activate or configure the biometric reader function on the mobile device, as recommended by the manufacturer of the device or the software installed on it,
   2) enter into the memory of this device one of his/her biometric characteristics, which will be the basis for the creation of the biometric identifier of the user,
   3) accept the authentication method based on a biometric identifier.
6. If the Bank considers that the technical or technological solution used by the manufacturer of the mobile device for the use of the biometric reader functionality poses a risk for the IT security of the Bank or its clients, the Bank reserves the right to refuse to authenticate the user on the basis of the biometric identifier. In that case, user authentication is performed according to the rules described in sec. 3 p. 1) and p. 2).
7. Where the user uses a trusted mobile device, the Bank assumes that all instructions given by means of that device have been given by the user, using the simplified authentication operation. Therefore, once a device is added to the list, the user is obliged to make sure that such a device is stored safely and is not made available to third parties. The list of types of instructions that are executed by the Bank on the basis of the user's authentication performed by linking him/her to the mobile device he/she has added to the list can be found in the Announcement.
8. Proper authentication of the user, carried out in accordance with sec. 2 and 3, will enable the user to access information on accounts or other services made available through the System and to give instructions with respect to those accounts and those products or services.
9. Failed user authentication when logging into the System, by entering an incorrect password five times in a row, results in automatic blocking of access to the System. The counter of failed login attempts is reset after a correct login.
10. Failed authentication of the user when logging into the Mobile Application by entering an incorrect PIN code three times in a row, results in blocking of the user and may result in blocking of access to the System. The counter of failed PIN code attempts is reset after a correct login. Reassignment of the PIN code is possible after correct entry of the password in masked form.
11. Where the user has used a biometric reader when logging into the mobile application and the user has not been authenticated on the basis of the biometric identifier, logging into the mobile application will be possible after entering the correct PIN code or other authorisation code.

5. Electronic transmission of declarations of intent and knowledge

Article 8

1. On the basis of the Agreement concluded, the user and the Bank may use the Internet Banking System to make declarations of intent or knowledge in electronic form, in connection with performance of
   1) banking activities, or
   2) other activities in accordance with the Bank's Articles of Association.

   Such declarations may be made subject to the provision that, due to the constant development of information technology, individual functionalities made available through the Internet Banking System may change or be made available at different times. Information concerning the possibility of making certain declarations of intent or knowledge at a given time is described in the Announcement.
2. Declarations of intent in an electronic form related to the performance of the activities referred to in sec. 1 p. 1) and p. 2) include declarations which are related to the establishment, performance, change, termination, dissolution or expiry of the legal relationships concerning these activities. Moreover, such declarations include the granting, amendment or revocation of a power of attorney related to the performance of the activities referred to in sec. 1 p. 1) and p. 2).
3. Insofar as electronic declarations of intent meet the legal requirements for being deemed to have been made in

writing, they will be deemed to have been made in writing, also in the cases when such form is mandatory for a declaration to be considered valid. In the case of instructions, including those requiring written form, the signature may be provided in electronic form if it complies with the requirements of an electronic form equivalent to a written form in accordance with the applicable legal provisions. Such an electronic signature may be affixed as a qualified electronic signature, advanced electronic signature or other electronic signature as defined by the generally applicable law, including:

1) by sending to the other party data identifying the user or the Bank, or

2) any other method permitted by law.

4. Insofar as legal regulations allow a given method of instruction authorisation to be recognised as an electronic signature, the user may provide such a signature for authorisation purposes. Where the Bank provides a signature in electronic form by sending identification data to the other party, the signature sent via the System contains data identifying the person representing the Bank. By virtue of declarations of intent submitted via the Internet Banking System, the Bank and the user may, by means of an annex to the agreement concluded in electronic form, introduce a different method of affixing a signature in electronic form if the law consider such method as satisfying the requirements of written form.

5. The Bank and the user may perform actions or conclude agreements/annexes to agreements or make declarations requiring written form in electronic form equivalent to written form. If permitted by law, the Bank and the user may use the System to make other declarations that require a written form in electronic form equivalent to a written form.

6. Where on the basis of the information, statement or document available in the System, it appears that the Bank's or the user's declaration of intent or knowledge relates to more than one instruction or more than one statement or document, a single electronic signature will be deemed to relate to all instructions or all statements or documents transmitted.

7. The Bank will send correspondence to the user, including any declarations of intent or knowledge, specimen documents, as well as agreements concluded by the user together with the general terms and conditions, and other documents by means of the Internet Banking System, unless generally applicable laws provide otherwise. Correspondence, including declarations of intent or knowledge sent by the Bank may bear a qualified electronic seal, an advanced electronic seal or another electronic seal prescribed by generally applicable law.

8. The Bank may enable the user to deliver correspondence to the Bank electronically via the System. Due to the development of information technology, the different types of declarations (correspondence) made available through the System may change or be made available at different times. Information on the possibility of making certain types of declarations (correspondence) at a given time is described in the Announcement.

9. The Bank will send the user electronically, including via the System, messages confirming the fact that a certain agreement has been concluded or that an instruction has been accepted for execution.

6. Electronic delivery of correspondence

Article 9

1. As part of the Internet Banking System, the Bank makes available to the user:

1) "message" box which is used to contact the Bank and the user,

2) the Electronic Correspondence Delivery System in which the Bank will publish changes to contractual regulations that are required by law to be delivered in a durable medium. The use of the name Electronic Correspondence Delivery System in other regulations applicable to the Bank's products and services means this service. The Bank will also include in the Electronic Correspondence Delivery System users' account statements, statements of credit card

2. The Bank will not be liable for the consequences of failure to read documents/messages/correspondence sent through the Internet Banking System. The user is obliged to read the messages sent to him/her by the Bank via the System. The above will be without prejudice to the Bank's right to send correspondence to the user by post to the address provided by the user or to deliver the correspondence to the user personally at the bank branch carrying out this activity.

3. As of the date on which the Electronic Correspondence Delivery System is made available by the Bank, changes

to contractual regulations, which by law must be sent on a durable medium, will be delivered by the Bank to users who are a party to the Agreement, in the Electronic Correspondence Delivery System. It will enable the user to store information addressed to him/her from the Bank in such a way that it can be accessed for a period of time adequate for the purposes of compiling the information and allowing the information stored to be reproduced unchanged. This space is an integral part of the System and may appear under different brand names. Access to it does not require a separate agreement.

4. The user will have access to the Electronic Correspondence Delivery System until the Agreement is terminated. Prior to the termination of the Agreement, the client may print or save on another durable medium the documents that have been delivered to him/her by the Bank in the Electronic Correspondence Delivery System.
5. Upon termination of the Agreement, the Bank will provide the user with access to the contents of the Electronic Correspondence Delivery System via the Document Archive (hereinafter: Archive), provided that the Bank makes such a possibility available, or provide such a user with the content of this system on another permanent information carrier.
6. Logging into the Archive requires the user to provide the Bank with their e-mail address and telephone number for authorisation. These data are necessary for the client to log on to the Archive.
7. When using the Archive, the user should observe the security rules provided for in the General Terms and Conditions. In the case of a suspicion that an unauthorised person has gained access to his/her Archive, the user will immediately block access to his/her Archive or change the data necessary for the use of the Archive (e-mail, telephone authorisation).
8. The Bank is entitled to block access to the Archive in accordance with the reasons for blocking the System. The user can also block access to the Archive himself/herself.
9. The user may submit an instruction to unblock the Archive or to change the login data for the Archive only at the bank branch carrying out this activity.
10. Details related to the user's use of the Archive are contained in the Announcement.

7. Submission of instructions, their authorisation and execution

Article 10

1. The Bank will execute instructions submitted only by users to whom it has assigned a login.
2. The user may not use the System to give the Bank instructions to perform payment services in connection with his/her participation in gambling games unless a game is conducted in accordance with the Gambling Act. The Bank has the right to refuse to carry out such instructions.
3. It will be possible to submit an instruction via the mobile application as long as a mobile device is on the list of trusted mobile devices at the time of submission.
4. The Bank has the right to set limits on the amount and quantity of payment transactions carried out on the basis of payment orders that are executed using the Internet Banking System.
5. For security reasons, the Bank may introduce a protection period for instructions submitted by the User in the System, which we describe in the General Terms and Conditions.
6. The Bank shall apply restricted access mode if the User activates it.
7. The User may set a transaction limit in the System. For new customers, the transaction limit is PLN 5,000. The limit is the same for both Internet and mobile banking. No more than once per quarter, the Bank may lower the transaction limit based on an analysis of the User's expenses. The Bank shall notify the User of any changes in the System. The User may change the limit at any time.

   The following are not included in the transaction limit:

   1) transfers between the payer's own accounts maintained by us,

   2) transfers to ZUS/Tax Office accounts.

   In the case of payment orders where the amount is expressed in a foreign currency, in order to determine the limit expressed in Polish zlotys (PLN), the amount expressed in a foreign currency is converted into Polish zlotys (PLN) according to the mean exchange rate of the National Bank of Poland (NBP) current at the time of receipt of

the payment order by us.

8. Where required by law, the Bank makes the execution of instructions, including payment orders, subject to strong authentication of the user. In the event that the Bank requires that the strong authentication of the user takes place via the mobile application, the user is required to have a trusted mobile device when performing a given action.

Article 11

1. The Bank executes payment transactions after they have been authorised by the user. Authorisation of a payment order by the user implies his/her consent to make the payment transaction. Consent to make a payment transaction may also be given by the user through the payee, the payee's provider or the provider initiating the payment transaction.
2. Authorisation of instructions, including payment orders submitted by the user via the Internet Banking System, including the mobile application, includes:
   1) select the accept button – when the Bank considers that a given instruction may be authorised in this way due to security rules, or
   2) select the accept button in the mobile application (mobile authorisation) – when the Bank considers that a given instruction should be authorised using the mobile application. This method of authorisation also requires that the user is in possession of a tangible trusted mobile device on which the mobile application is installed and activated, or
   3) enter the correct authorisation code(s), including the biometric identifier and select the accept button – when the Bank considers that a given payment instruction, due to the provisions of law or security rules, should be authorised by entering an authorisation code(s), or
   4) enter the correct authorisation code(s), including the biometric identifier and bring the mobile device into proximity of a terminal, or
   5) the use of a security key when the user has an active key on the list of security keys and when the Bank considers that a given instruction, due to security rules, can be authorised in this way or
   6) the use of a physical payment card, with contactless payment enabled, by bringing it close to a mobile device with the mobile application installed and NFC enabled.
3. In order to authorise an instruction with a biometric identifier, the user should first
   1) activate or configure the biometric reader functionality on the mobile device, as recommended by the manufacturer of the device or the software installed on it,
   2) enter into the memory of this device one of his/her biometric characteristics, which will be the basis for the creation of the biometric identifier of the user, and agree to an additional authentication method and a method for authorising instructions with the biometric identifier.
4. For security reasons, the Bank reserves the right to refuse to authorise an instruction made on the basis of a biometric identifier. The reason for this may be that the Bank considers that the technical or technological solution used by the mobile device manufacturer for the use of the biometric feature reader functionality poses a risk to the IT security of the Bank or its clients. In this case, the authorisation of the instruction is carried out in accordance with the rules described in Article 11 sec. 2, with the exception of the possibility to use the biometric identifier for this purpose.
5. Every instruction given by the user, which is to be executed by the System and which will cause a change in the cash balance on the accounts, or which will constitute an application for the Bank to conclude a new agreement or perform a service, or will be related to such an application, must be authorised by the user in accordance with Article 11 sec. 2.
6. Authorisation of an instruction with a security key requires the user:
   1) to register the security key in the online banking system,
   2) to activate the security key at a bank branch or the bank's call centre, or through the internet banking system, if the bank offers such a possibility, and to agree to such an authentication method.
7. Applying security principles, the Bank verifies that the user is authorised when submitting instructions by:
   1) checking the correctness of the data provided by the user when logging into the System, as referred to in

Article 7 sec. 2 and 3,

2) checking if the user selected the accept button for an instruction, which was recognised by the Bank as not requiring authorisation by providing an authorisation code,

3) verification of the correctness of the authorisation code or codes provided by the Bank and given by the user, including the biometric identifier or verification of the use of the security key, if the user has an active key on the list of security keys.

If the result of the verification referred to above is negative, the Bank considers that the instruction is not authorised by the user and refuses to execute it.

8. The Bank provides the user with authorisation codes, which are text message codes, in a text message sent to the telephone number previously indicated by the user for authorisation.

9. The validity period of an authorisation code provided by the Bank may be limited for System security reasons. The standard validity time is limited to the duration of a session, i.e. the time the user is connected to the Bank via the System. The authorisation code is generated for a submitted instruction and can only be used to authorise that instruction. Together with the authorisation code, the user receives information about the details of the instruction.

10. If an incorrect authorisation code provided by the Bank for the approval of a given instruction is entered five times, access to the Internet Banking System is blocked. If the user enters an incorrect PIN code three times to approve an instruction in the mobile application, the Bank may block access to the Internet Banking System.

11. An instruction to unblock access to the System may be given at a bank branch carrying out this activity, via the Bank's website or in the mobile application, provided that the Bank allows such functionality. In each case, the user must re-set the password or PIN code for the mobile application to unlock.

12. For security reasons, the Bank reserves the right to request additional authorisation for any instruction, e.g., using authorisation codes or security keys, if the user has an active key on the list of security keys.

Article 12

1. An instruction given by the user in the Internet Banking System is an irrevocable and final expression of the user's intent, subject to sec. 5.

2. Instructions given via the System may only relate to accounts and banking products or services available to the user via the System.

3. Information on the procedure for the execution of individual instructions submitted using the Internet Banking System is available in appendix 1 and on the Bank's website, in the section concerning the System.

4. The moment the Bank receives a payment order submitted via the internet banking system

1) on a business day or on Saturday before the cut-off time set out in appendix 1, subject to item 3) below, will be the moment when the payment order is authorised in accordance with Article 11 sec. 2,

2) on a business day or on Saturday after the cut-off time set out in appendix 1 or on a public holiday, subject to item 3) below, will be the first business day following the day on which the payment order was submitted, with the exception of payment orders indicated in appendix 1 for which there are no cut-off times for receipt of payment orders, and for which the moment of receipt of the payment order will the moment defined in 1) above,

3) with a deferred payment date (a transfer executed on a day other than that on which the payment order is submitted):

a) will be the date indicated by the user for debiting his/her account;

b) if the day indicated by the user for debiting the account is not a business day (except for Saturday), the payment order will be deemed to have been received on the first business day following the day indicated by the user for debiting his/her account, subject to the orders mentioned in item c) below;

c) if the day indicated by the user for debiting his/her account is not a business day (except for Saturday), then for payment orders set out in appendix 1 for which there are no cut-off times for receipt of payment orders, the time of receipt of such payment orders by the Bank will be the day indicated by the user for debiting his/her account;

d) if the day indicated by the user for debiting his/her account falls on a Saturday, the payment order will be deemed to have been received on that day, subject to the orders set out in item e) below;

e) if the day indicated by the user for debiting his/her account falls on a Saturday, then for payment orders set out in appendix 1 for which there are cut-off times for receipt of payment orders, the time of receipt of such payment orders by the Bank will be the first business day following the day indicated by the user for debiting his/her account.

5. Subject to sec. 6, a user may not revoke a payment order from the moment it is received by the Bank, unless other general terms and conditions or separately concluded agreements provide otherwise.

6. In the case of an outgoing payment order defined in appendix 1, the user may cancel it before the day and time set out in appendix 1.

7. Where a payment transaction is initiated by or through a provider of payment transaction initiation services or by or through a payee, with the exception of a deferred payment order as defined in sec. 4 p. 3), the payer may not cancel the payment order after having given his/her consent for the provider of payment transaction initiation services to initiate the payment transaction.

Article 13

1. The Bank will execute instructions, including payment orders submitted via the Internet Banking System on the rules provided for in the General Terms and Conditions, and in matters not regulated herein, on the rules provided for in separate regulations binding on the user regarding the relevant accounts or other services to which the instruction in question relates.

2. In the case of termination of the Agreement, a deferred payment order previously submitted via the System will be executed in accordance with the instruction submitted.

3. Subject to sec. 5, the Bank refuses to execute an instruction, including a payment order, for reasons indicated in the agreement or in the general terms and conditions, which are binding on the user and apply to the relevant account, and furthermore an instruction which:

1) is incomplete or incorrect due to an incorrect unique identifier or other incorrect information required to execute the instruction,

2) is contrary to another instruction previously submitted,

3) cannot be executed due to insufficient funds in the account concerned,

4) is unauthorised, as described in the General Terms and Conditions,

5) for other reasons expressly provided for in the General Terms and Conditions, the Agreement or the generally applicable law.

This applies to all payment orders, including those initiated by or through a payee.

4. The user will promptly receive a notification of refusal to execute an instruction via the System. Where possible, he/she will also be informed of the reasons for the refusal or the procedure for rectifying the errors that led to the refusal, unless such notification is inadmissible under separate legislation.

5. In the event that the person submitting the order in the Internet Banking System fails to update his/her identity document with the Bank, the Bank has the right to refuse to execute the payment order.

6. The Bank will execute payment transactions on the same basis irrespective of whether the payment order was submitted by the user directly to the Bank or was initiated by the provider of payment transaction initiation services unless the provisions of the General Terms and Conditions provide otherwise.

Article 14

Information required by law will be made available periodically, at least once a month, free of charge in the System – unless otherwise set out in a separate binding regulation or the General Terms and Conditions.

Article 15

1. If the user submits an instruction which is a payment order at a bank outlet providing this service or via the helpline, the user may, if the Bank makes such a possibility available, authorise such an instruction by giving at that outlet or via the helpline the authorisation code received by means of a text message sent by the Bank to the user's telephone number for authorisation or authorises such an instruction in the mobile app.

2. If the user submits an instruction which is not a payment order at a bank outlet providing this service or via the helpline, the user may, if the Bank makes such a possibility available, submit such an instruction, with the

reservation of instructions which in accordance with the General Terms and Conditions can only be submitted in writing or via the Internet Banking System, by giving at that outlet or via the helpline the authorisation code received by means of a text message sent by the Bank to the User's telephone number for authorisation or authorises such an instruction in the mobile app. The list of instructions is defined in the Announcement.

3. If the Bank makes such a possibility available, the user may submit an instruction which is a payment order or an instruction which is not a payment order and authorise it by affixing a signature on an electronic device at a bank outlet providing this service, in accordance with Article 7 sec. 1 of the Banking Law, after providing the Bank with his/her identification data and having the identity of the person making the statement confirmed by a Bank employee. The documents on the basis of which the Bank confirms identity are set out in the Announcement for holders of accounts set out in the General Terms and Conditions for the provision of services by ING Bank Śląski S.A. as part of the framework of maintaining an Account for Refugees. The electronic device will ensure the recording and integrity of the content of the declaration, the signature affixed and the date and time of the declaration. If the client's declaration of intent is related to the establishment, performance, change, termination, dissolution or expiry of legal relations binding him/her with the Bank and requires the Bank to make a declaration of intent, the Bank will affix an electronic signature by including in its content the identification data of its representative, i.e. the employee's first and last name and identification number.

8. Financial management support services

Article 16

1. As part of the System, the Bank provides services to support financial management (hereinafter: financial management). These services are of a consultancy and advisory nature and relate in particular to payments.
2. The Bank, in order to provide these services, makes the System functionalities available which are adapted to the individual needs of the user. In order for the Bank to perform financial management, it is necessary to categorise financial information and profile personal data concerning the user within the meaning of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 – General Data Protection Regulation. Profiling may only take place to the extent necessary to perform financial management. When performing financial management, the bank does not make decisions on financial matters for the user.
3. Financial management does not include advisory services, portfolio management, preparation of investments, financial analysis and other recommendations within the meaning of Article 69 sec. 2 and sec. 4 of the Act on Trading in Financial Instruments, which may be provided by the Bank on the basis of other agreements/regulations, even if they are provided remotely via the System.
4. Financial management is provided in the form of:
   1) information or notifications about:
      a) financial terminology and knowledge in these fields,
      b) future payments, including those made periodically by the user and future events or dates,
      c) possible future payments by the user, including periodic payments,
   2) the presentation of the user's financial situation by indicating:
      a) the type of transactions carried out by him/her or whether the transactions belong to a specific group or type of transactions,
      b) the type or category of receipts, expenses or business counterparties,
5. The information, presentations and consultations referred to in sec. 4 may be provided in a variety of visual or textual forms.
6. Financial management will be performed in accordance with the following principles:
   1) information concerning terminology is provided in the System on an ongoing basis, while notifications of future transactions/events or deadlines are provided no later than 48 hours prior to the transaction/event or deadline indicated in the System,
   2) the presentation of the financial position will be prepared on a monthly or annual basis, on the basis of payments made or expected to be made. These presentations may also take into account information provided by the user on the System or by others acting under the authority of the user. The system may allow a different setting of the period of a given presentation.

7. Financial management is an integral part of the System, except that within these services individual functionalities may need to be activated by the user themselves.

Article 17

1. For the due performance of financial management, the Bank will be liable for proven losses of the user, subject to sec. 2.
2. The Bank will not be responsible for the purpose, undertaking or limit of expenditure set by the user, nor for their execution or level of execution.
3. The Bank is not responsible for any financial management decisions made by the user, including decisions to purchase particular services or to invest funds. This exclusion of liability does not cover situations where the Bank has breached its duty to act with due diligence, nor does it contravene mandatory provisions of law.
4. The Bank will prepare the consultation to the best of its will and knowledge and with due diligence, based on the facts known to the Bank existing at the time the consultation is provided, in particular on information provided by the user. The Bank does not verify whether the information provided by the user is correct. In order to obtain a reliable consultation, the user must provide truthful information, in particular on his/her financial situation.
5. Where, as part of financial management, a particular functionality is activated by the user himself, the Bank – irrespective of its information obligations under the law – may provide additional information on the risks associated with the services. It is the user's responsibility to read this information and to make decisions regarding the investment of funds reasonably.
6. Due to the continuous development of information technology, individual functionalities made available within the framework of financial management may change or may be made available in the System at different times. Information on their availability can be found in the Announcement. These functionalities may have different designations and names.
7. Financial management is provided until the expiry or termination of the Agreement. After this moment, the user does not have access to the results of the financial management support services prepared by the Bank, in particular information, presentations, consultations and financial objectives or undertakings that the user has set. Before the date of expiry or termination of the Agreement, the user may print out the results of the financial consultation or save them and store them on electronic media – provided that the System enables preparation of the consultation in the form of a text file.

9. Digital vault in the internet banking system

Article 18

1. Digital vault (hereinafter: vault) is a service which consists in storing electronic documents (also known as files) saved by the user) in a dedicated separate space of the Internet Banking System. This space is an integral part of the System and may appear under different brand names.
2. The Bank will make the vault service available to users who have concluded the Agreement. The use of this service does not require a separate agreement. In the vault space, the user can save files, download or delete previously saved files. The user will not be able to edit saved files or change their formats.
3. The catalogue of file formats that can be saved in the System is given in the Announcement.
4. The user obtains access to the vault at the moment of logging into the System. The user may use the vault only when logged in to the System.
5. The vault is linked to the user's login. If the user has several logins, the service is available separately for each login. It is not possible to use the same vault under several logins.
6. Information on the available capacity of the vault is given in the System.
7. The user is responsible for the content of the saved files and their format. The user may only store in the vault the files to which he/she is entitled, which do not infringe the provisions of commonly applicable law, have been created or obtained in accordance with the law and do not infringe the rights of third parties, including personal rights, copyrights, industrial property rights or trade secrets of these persons. The user may only save files which do not contain any electronic viruses or any parts of dangerous software.
8. The Bank has the right to refuse the user permission to store in the digital vault a document that does not meet

the technical requirements, would pose risk to the security of the Bank, the Bank's electronic systems or other users, or funds collected at the Bank. As soon as the Bank becomes aware of a breach of Article 27 sec. 7, it will refuse to allow the user to upload files. In the event that a breach of security or infringement of the obligations indicated in sec. 7 could lead to a serious loss for the Bank or other users, the Bank has the right to launch appropriate security software and, in cases of urgent risk, to isolate or, if this is not possible, to delete the stored files.

9. The Bank does not have access to the files and documents uploaded by the user into the vault and does not check or verify the data and content of the files and documents. The scope of the Bank's liability from the time a file is saved in the vault is defined in the General Terms and Conditions

10. When storing files saved by the user with due diligence, the Bank will not be liable for:

1) the content of and data included in files and documents uploaded to the System,

2) a change of a file name by the user,

3) files retrieved from the vault at the time of submitting an instruction,

4) the consequences of any breach by the user of the rights described in sec. 7 or sec. 8,

5) leaving a file in the vault upon expiry or termination of the System agreement,

6) losses and costs incurred as a result of any damage to the file, its complete damage or interception of the file during its transfer to the System, unless these resulted from the operation of the Bank's IT system,

7) failure of the Bank to detect, at the time the file is saved to the System, any virus-infected elements,

8) delay in carrying out or failure to carry out the user's instructions submitted as part of the vault service where this is due to force majeure.

11. The Bank will make the contents of the vault available to authorities authorised by law, without analysing the files contained in it, in accordance with the procedure laid down in the relevant provisions of the Banking Law.

12. The Bank will not be liable for any losses resulting from the disclosure of the contents of the vault to persons or institutions authorised to request such information from the Bank.

13. The user will lose access to the vault and the files/documents stored therein upon expiry or termination of the Agreement. When the System is closed, the files/documents stored in the vault are automatically and permanently deleted by the Bank. The Bank does not keep copies of these files/documents. Prior to termination of the Agreement, the Bank will notify the user to download the saved files. Notification may be made by any means, including by a message displayed to the user in the System.

14. For technical reasons, the development of technology and software used to operate the vault or for security reasons, the Bank has the right to restrict the use of the storage of certain file formats in the vault space or to limit the functionality of the vault. In such a case, the user will be informed in the System before a certain action is performed.

10. Use of payment services provided by authorised third parties

Article 19

1. The user may, to the extent permitted by the authorisations held, make use of third party payment services such as those providing access to account information or the payment transaction initiation service:

1) access to account information service – performed by a provider of access to account information service, consists in sending by the Bank – upon request of this provider – information on the account kept in the Bank;

2) payment transaction initiation service – performed by the provider of the payment transaction initiation service, consists in the initiation by this provider, acting at the user's request, of a payment order from a payment account held with the Bank to which the user is entitled.

2. The use of the access to account information service is possible on condition that the account maintained by the Bank is a payment account available on-line and the user is authenticated by the Bank, in accordance with legal requirements and the provisions of the General Terms and Conditions.

3. The use of the service of payment transaction initiation is possible on condition that, in accordance with the regulations binding on the user, it is a non-cash electronic transaction relating to a payment account available online, its initiation is effected solely as a result of the user's instruction, and furthermore that the user is

authenticated by the Bank, in accordance with legal requirements and the provisions of the General Terms and Conditions.

4. The Bank will make available to an account information service provider information on indicated accounts and related transactions, including the history of such accounts – except that the period for which the Bank provides account history may be limited for technological reasons.
5. The Bank will not be liable for the proper performance of the services referred to in sec. 1 by authorised third parties.
6. The user may give permission in the System for the Bank to respond to requests from providers issuing payment instruments based on a payment card, confirming that the amount of a specific payment transaction executed using that card is available on the payment account.
7. A payment account will be available online when all the following conditions are met:
   1) the user is a party to the Agreement,
   2) the user has active access to the Internet Banking System,
   3) the payment account in question is available via the System upon receipt by the Bank of an appropriate application or request from the relevant provider to perform an action in order to provide the service mentioned in sec. 1.
8. A payment account is not available online when at the moment the Bank receives an appropriate application or request for action:
   1) the user does not have an active Internet Banking System, or
   2) when access to the System is blocked, or
   3) where the user has used the function of hiding a given account from the System and has not revoked this instruction.
9. The Bank may refuse a provider of the access to account information service or a provider of the payment transaction initiation service access to a given payment account for objectively justified and duly documented reasons relating to unauthorised or illegal access to the payment account by such a provider, including unauthorised initiation of a payment transaction. In such a case, the Bank will inform the user via the System of the refusal of access to the payment account and the reasons for it. Such information will, where possible, be communicated to the user before such refusal and at the latest immediately thereafter, but not later than on the business day following such refusal, unless its communication would be inadvisable for objectively justified security reasons or is contrary to separate legislation.

11. Liability of the Bank

Article 20

1. The Bank agrees to:
   1) maintain the confidentiality of all user authentication and authorisation data,
   2) provide the user with access via the Internet Banking System to current information on the accounts to which he/she is entitled in such a way as to enable him/her to monitor transactions effected on such accounts on an ongoing basis.
2. The Bank will be liable for proven losses of the user caused by the non-execution of an instruction or its incorrect or untimely execution unless they are a consequence of circumstances for which the Bank is not responsible.
3. The Bank shall be liable for any consequences of transactions executed by third parties after the notification referred to in Article 22a(4) and (5) has been made and the user has submitted an instruction to block access to the System or activated limited access to the System, starting from:
   1) receipt of the instruction by the Bank – if the instruction was submitted via the System,
   2) a written confirmation by the Bank of the fact that such an instruction has been given – if the instruction is given at a bank outlet performing this service;
   3) the user obtains an oral confirmation of blocking of access to the System from the helpline – if the instruction was given via the helpline,

   unless the user has intentionally caused an unauthorised transaction.

4. The Bank is liable for protecting the confidentiality of the user's data used for authentication and authorisation by means of the Internet Banking System only if the user uses such data in accordance with the principles set out in the General Terms and Conditions unless confidentiality has been breached through the Bank's fault.
5. The Bank will not be liable for non-performance or improper performance of the Agreement where the reason for non-performance or improper performance of the Agreement, including transactions, is force majeure.
6. The Bank will not be liable for non-performance of the Agreement where the refusal to perform obligations under the Agreement is based on generally applicable laws that authorise or oblige the Bank to refuse to perform such obligations or instructions.
7. The Bank will not be liable for:
   1) unexecuted instructions – in the case of incorrect or incomplete information concerning the unique identifier or a failure on the part of the payer or payee to provide the information necessary for the execution of a given instruction or transaction, to the extent that the failure to execute the instruction results from a failure to provide the information necessary for its execution,
   2) consequences resulting from the operation of the user's telecommunications equipment in connection with the receipt of text messages, provided that the delay in receiving a message was not the fault of the Bank,
   3) user's losses caused by the user's failure to comply with the security rules of the Internet Banking System.
8. In relation to users who are a party to a payment account agreement within the meaning of the Act, the Bank will be liable for non-execution or improper execution of a correctly ordered transaction, unless it proves that the payee's account was credited within the period required by law or when:
   1) the user's claims are extinguished as a result of failure to report, within the 13-month period required by the General Terms and Conditions, the unauthorised, non-executed or inadequately executed transactions, or
   2) the non-execution or improper execution of the transaction was due to force majeure or was due to the provisions of law.
9. Where, in accordance with the General Terms and Conditions, the Bank is liable to the payer or the payee who is a user – it undertakes to reimburse him/her for the amount of the non-executed or improperly executed transaction, and where such user is a payment account holder within the meaning of the Act – to restore the account to the state it would have been in had the improper execution or non-execution of the transaction not occurred. The same will apply to fees or interest charged to the user in case of non-execution or improper execution, including late execution, of a payment transaction.
10. In the case of a non-executed or improperly executed payment transaction initiated by or through the payer or the payee, the Bank will, at the request of the payer or the payee, immediately take steps to trace the payment transaction free of charge and, where permitted by law, notify the payer of the outcome.
11. Matters not regulated in the General Terms and Conditions, which concern the Bank's liability for the execution of payment orders, including payment transactions initiated through the provider of the payment transaction initiation service and requests for reimbursement of amounts of unauthorised transactions, will be governed by the provisions of the General Terms and Conditions for the provision of services by ING Bank Śląski S.A. as part of the framework for maintaining an Account for Refugees.
12. In providing the Internet Banking System service in accordance with these General Terms and Conditions, the Bank will exercise due diligence as defined in the Civil Code.
13. The Bank is not liable for the security and operation of the trusted mobile device, including any of its functions.

Article 21

All instructions given by the user via the Internet Banking System are secured permanently by the Bank and constitute evidence in case of disputed situations.

12. Liability of the User

Article 22

1. In providing the Internet Banking System service in accordance with these General Terms and Conditions, the Bank will exercise due diligence as defined in the Civil Code.
2. The Bank is not responsible for the security and operation of the trusted mobile device, including all its functions.

Article 22a

1. The user agrees not to take any action that would result in a third party gaining access to the System, even if it is another user.
2. The user is obliged to comply with the following rules for the use of the System:
   1) to keep confidential all data and information used to:
      a) to authenticate and authorise all (payment or non-payment) instructions (e.g. login, codes, password, PIN) which are used to use the System or any part thereof,
      b) to use the System, the My ING application or any of their functions or features.

   This data and information must not be disclosed by the user to a third party, even if that person is another authorised user of the services through the System,
   2) to memorise his/her password or other data used for authentication and authorisation and, if he or she is unable to do so, store that password and data in a secure manner of his/her choice and in a secure location that is not accessible to third parties. The user is obliged to store login, authentication or authorisation devices (e.g. U2F key) in the same way. It is unacceptable to store the password and the data that enable authentication or authorisation together in one place (e.g. storing the password together with other data,
   3) the user is obliged not to make available to a third party a trusted mobile device which would have the effect of enabling a third party to obtain authentication or authorisation data or to submit instructions to the System,
   4) the user is obliged:
      a) not to install or permit to be installed any software or tool on your trusted device or other device you use to connect to the System that will enable a third party to access the System, and
      b) not to connect your trusted device or any other device you use to connect to the System with software that will enable other persons/entities to gain access to the System, including taking control of your device or directing its functions (any means of impersonating you),
   5) the user is obliged to protect the trusted device and the devices the user uses to connect to the System (e.g. computer, mobile phone, other mobile devices) from malware or third party access by:
      a) installing only legal software on the Trusted Device and other devices from which it connects to the System,
      b) installing anti-virus software, except that it may be free of charge on the Trusted Device and other devices from which it connects to the System,
      c) establishing a code, password or PIN or other security measure for access to a trusted device or other device from which the user connects to the System,
      d) not allowing the storage of third party biometric features on a trusted or other device used for authentication or authorisation, e.g. facial features (face ID function) or fingerprints, vascular images (touch ID function), as this creates the risk that the device could classify the third party's data as user data,
   6) the user is obliged to install updates (including new versions and patches) of the mobile application on a regular basis – no later than the dates specified by the Bank. In the event that an update, new version or patch is critical, the Bank notifies the user to install it, implement it immediately before logging in. Furthermore, if the user has installed a mobile application or continuously uses the same device while using the System, the user is obliged to regularly update and install patches and new versions, at least of the operating system software (e.g. Android, iOS), which are recommended by the device or software manufacturers, if the respective manufacturer provides such support. Failure to install current versions or patches of the above may affect the security of the System.
3. The user will comply with the following rules relating to authentication and authorisation of instructions:
   1) before each authorisation, the user is obliged to check whether the instruction is in accordance with the user's intention, and if the user receives information from the Bank before the authorisation, he/she is obliged to familiarise himself/herself with this information. If the instruction is to add a device to the list of trusted devices, the user should make sure that he or she actually owns the device (actually wields the device) before

submitting the instruction,

2) the user is obliged to notify the Bank immediately of any unauthorised, incorrectly initiated, non-executed or improperly executed payment transactions resulting from instructions submitted through the System. This notice can be given by the user via the System, by telephone via the call centre or at a bank branch,

3) if the user intends to use an authentication or authorisation method based on a biometric identifier, he/she will be required to use only one of his/her own biometric feature which will be the basis for the creation of the biometric identifier. If the mobile device allows recording multiple copies of a biometric feature (e.g. several fingerprints), the user is required to register only one of their own biometric features, as this feature will subsequently be assigned to the user key referred to in Article 1 sec. 2. p. 8).

4. The user is also obliged to immediately report the loss, theft to the Bank, misappropriation or unauthorised use of authentication or authorisation data by the System, as well as unauthorised access to the System.

5. The user is obliged to notify the Bank immediately in the event of identifying:

1) loss, theft, misappropriation or discovery of the unauthorised use of a trusted device or a mobile phone or other device that is associated with a telephone number marked as a telephone number for authentication or a log-on, authentication or authorisation device (e.g. U2F key),

2) any technical incident or other failure related to the use of the System which, in the opinion of the user, may compromise the security of the System or the safe use of the System by the user,

3) that third parties have attempted to log into the System. There is also an obligation to notify the Bank immediately if there is a suspicion that there has been a breach of security or of the individual authentication data used by the user, such as codes, authorisation codes or biometric identifiers.

6. In the cases referred to in sec. 4 or 5 and in the event of disclosure or suspicion, that authentication or authorisation data have been disclosed to third parties instructions or access to the System by other persons, the user should immediately:

1) notify the Bank and block access to the System or instruct the Bank to block access to the System. An instruction to block the System may be given at the bank branch carrying out this activity, via the System or via the call centre.

2) change any authentication or authorisation data that is capable of being changed.

7. In the event that the user finds that:

1) a crime has been committed, including identity theft, or an action resulting in access to the System by an unauthorised person, or

2) there has been the use by a third party of other payment instruments or data to which access is provided by the System or any part thereof, or

3) the acquisition by third parties of biometric features or biometric identifiers recorded on a trusted mobile device may lead to unauthorised access by such persons to the mobile application and unauthorised authorisation of instructions, the user will be obliged to take the steps provided for in sec. 5 without delay and to block the relevant data or payment instrument numbers with the relevant institutions. Furthermore, in the event of a suspected crime, the user is obliged to notify the competent authority, in particular the Public Prosecutor's Office or the Police.

8. The provisions on third-party access to the System do not apply:

1) where the provider providing the payment transaction initiation service or the provider providing the account information access service acts on behalf of the user, provided that those providers are acting with the user's consent for the purpose and to the extent of carrying out those services,

2) where the other user of the System is a minor on behalf of whom the user who is the legal representative of that minor has entered into an agreement for the System. The above is without prejudice to the rule that each user may only give instructions of his/her own, and a minor may only give instructions to the extent that he or she is authorised to do so by his/her legal representative or entitled by law.

9. In order to limit the risk of the user using websites similar to the Bank's website, the user is obliged to check when logging in whether the page displayed has the Bank's website certificate. The method of verification of this certificate is publicly available information and is stated on the Bank's website and on the login page of the Bank System. For information, we provide the current name of the Bank's website – www.ing.pl. The name of the site is subject to change, the Bank will announce it in the Announcement.

10. The user should not:

1) log in from a trusted device or any other device that he/she continuously uses when using the System to websites that are flagged as unsecure or unsafe (in such cases, software manufacturers also follow the practice of displaying a message on the user's device next to the name of the searched website, e.g. „the connection is not secure" or a sign/mark „!"),

2) indiscriminately allow applications installed on a trusted device or a device that the user uses on a regular basis while using the System to access other applications, as well as their photos, videos or contacts, – as such practices increase the risk of unauthorised access to a trusted device or a device that the user uses on a regular basis while using the System.

11. The user may provide the notifications or notifications referred to in the General Terms and Conditions through the System, by telephone via the call centre or at a banking facility.

Article 22b

1. The Bank recognises the user's report of an unauthorised transaction by carrying out a comprehensive investigation of the circumstances surrounding the transaction. The purpose of the test is to determine whether the user's instruction was correctly submitted and authorised by the user. The examination also includes determining whether the instruction is a user instruction or whether it was made by a third party, also made by means of software or another device.

2. If it turns out that the consent to execute the transaction was not given by the payer, it is deemed that such an instruction was not authorised. The above will be without prejudice to the liability rules described in these Rules.

Article 22c

1. If the user breaches one or more of the obligations described in Article 22a, it is assumed that the user is not using the System in accordance with the Terms of Use.

2. The user will be liable for unauthorised transactions to the full extent if they were the result of an intentional or grossly negligent breach of at least one of the user's obligations pursuant to Article 22a sec. 1-9.

3. With the exception of the provisions of section 2, the user is liable for unauthorised transactions up to the amount of EUR 50, converted at the average exchange rate of the euro published by the NBP, in force on the day of the user's transaction resulting from:

1) the use of lost or stolen authentication and authorisation data,

2) the misappropriation of authentication or authorisation data by a third party.

3) The user will not be liable for unauthorised transactions where:

4) he/she had no way of ascertaining the loss, theft or misappropriation of the authentication and authorisation data prior to the execution of the transaction, except where the user acted deliberately, or

5) the loss of data used for authentication and authorisation prior to the execution of the transaction was caused by an act or omission on the part of the Bank or entities indicated in Article 6(10) in the act on payment services.

4. With the exception of the situations described in sec. 2 and 3, in the event of an unauthorised transaction, the Bank will reimburse the amount of the unauthorised transaction to the payer immediately – but no later than by the end of the business day following the day on which the unauthorised transaction was discovered or the day on which the notification was received – except where the Bank has reasonable and duly documented grounds to suspect fraud and informs, in writing, the authorities appointed for the prosecution of crimes. Where the payer uses the payment account and a refund according to the above rule is due, the Bank will restore the debited account to the state it would have been in had the unauthorised payment transaction not taken place.

5. The payer will not be liable for unauthorised transactions after reporting to the Bank the loss, theft, misappropriation or unauthorised use of data used for authentication or authorisation by the System, as well as unauthorised access to the System as referred to in Article 22a sec. 4, unless he acted intentionally.

6. If the transaction was unauthorised and the Bank did not require the user to have strong authentication, the user is not liable for unauthorised payment transactions unless the user acted intentionally. The foregoing will not apply if the Bank was entitled under the law to waive the requirement for strong authentication. In the event that the payee or the payee's provider does not accept strong user authentication, they will be liable for the loss

suffered by the Bank.

7. Notwithstanding the above provisions, if the user fails to notify the Bank of unauthorised, improperly initiated, unexecuted, or improperly executed payment transactions within 13 months from the date the account was debited or the date the transaction was supposed to be executed, the user's claims related to unauthorised, unexecuted, or improperly executed payment transactions will expire.

Article 22d

1. If the user breaches one or more of the obligations set out in Articles 22 or 22a and if, as a result of this breach, it is found that:
   1) a third party – using all or part of the user's authentication or authorisation data – has made or authorised a non-payment instruction, and the Bank has executed that instruction or made a corresponding declaration (e.g. on the conclusion of an agreement), and
   2) the Bank has suffered damage as a result of the execution of the instruction or the submission of the corresponding declaration, because the instruction did not originate from the user,

   then the user will be liable for compensation for damage caused to the Bank as a result of the breach of the obligations provided for in Articles 22 and 22a according to the degree of breach of these obligations.
2. The user's liability will be limited to the Bank's actual damage resulting from the breach of the obligations provided for in Articles 22 and 22a. The user's liability does not exclude the Bank from seeking compensation from a third party until the damage is fully covered.

13. Other principles and recommendations for the safe use of the system

Article 23

1. The Bank will notify the user of current threats, i.e. the occurrence of fraud or suspected fraud or other threats to the security of the use of the System. These notifications may be:
   1) communicated to the user prior to logging on to the System,
   2) communicated to the user within the System (e.g. after logging in, in messages),
   3) transmitted via another secure communication channel agreed between the user and the Bank.

   In addition, information on this matter is published on the Bank's website.
2. The user will read the alerts on hazards referred to in sec. 1 and follow the recommendations indicated therein. Failure to familiarise yourself with risk alerts and to follow recommendations may involve risks, among other things:
   1) the occurrence of socio-technical attacks in which third parties, impersonating the Bank or another institution, may induce the user to provide identification data, authorisation codes or PIN codes
   2) the authorisation by the user of an instruction which he/she did not prepare,
   3) the use of equipment over which third parties have taken control.
3. Users are advised to ensure that their computer environment and mobile device environment is secure. The user is obliged to apply the Bank's current recommendations regarding the security of Internet transactions in order to protect himself/herself against specific threats caused by connecting to the Internet. These recommendations are presented by the Bank on its website. Information on subsequent updates of these recommendations is sent by the System.
4. The Bank applies security measures that reduce the risk of unauthorised use of the mobile application. Accordingly, the Bank is entitled to use electronic mechanisms to check whether the user or a third party has made changes to the trusted mobile device or to the original manufacturer-required software that has been installed on the device. It is recognised that making the changes mentioned above may result in the risk of an unauthorised person gaining control of the device.
5. If the Bank determines that there is a risk of an unauthorised person taking control of a trusted device, it may reduce the transaction limit for payment orders in the mobile application executed using that device – to not less than 95% of the limit amount set in the General Terms and Conditions. The Bank will notify the user of this without delay. The Bank has the right to block the System in accordance with Article 27 sec. 2 if the risk

mentioned above becomes high or the Bank determines that subsequent payment instructions or other instructions are submitted from a device which with great likelihood has become controlled by an unauthorised person, which would lead to unauthorised third party access to accounts, products or banking services through the System.

Article 24

1. The Bank publishes information on the safe use of the System on its websites and within the System. For details on where to publish safety information and recommendations, see the Announcement.
2. Logging into and using the Internet Banking System at your request requires cookies or other technologies that originate from the System. The Bank uses cookies and other technologies in accordance with the Cookie Policy (referred to as the Cookie Policy). In the Internet Banking System cookies and other technologies are used to establish and maintain the user session in the System, to support the protection of the integrity of the transactions and to identify the technical and technological characteristics of the device used when using the services of the System, in connection with the security requirements of the System and the transactions performed. In the event that the user uses the Bank's website but not the Internet Banking System, the user may, in accordance with the Bank's Cookie Policy, set its own web browser so as not to accept cookies other than those used in the System. The Cookie Policy applied by the Bank is available on the Bank's website.
3. The user is obliged to immediately notify the Bank of any changes to the personal data, and contact details of the user. A change of data may be submitted by means of the Internet Banking System, provided that there is a technical functionality in the System allowing for such a change of data. Except when the user serves a document in the form of a notarial deed, the authenticity of the user's signature must be certified:
   1) by a notary public – in the case of documents signed in the Republic of Poland;
   2) by a Polish diplomatic mission, consular post or notary of a country with which the Republic of Poland has signed an agreement on legal assistance in civil matters, or certified by an official or notary and provided with an apostille within the meaning of the Convention – in the case of documents signed abroad.
4. Subject to Article 24 sec. 5, instructions given by correspondence must be in the form indicated in Article 24 sec 3.
5. User statements and declarations mentioned in Article 29 sec. 1 and Article 31 sec. 3 may be submitted by correspondence without meeting the conditions defined in sec. 3. However, the Bank reserves the right to carry out additional verification of the statements and declarations submitted.

Article 25

1. The internet banking system may be unblocked by submitting an instruction at a bank outlet providing this service, by completing a relevant application on the Bank's website or in the mobile application, provided that the Bank allows such functionality. The user will be able to use the System once he/she has created a new password or PIN code to the mobile application.
2. The user can change the existing data required to receive authentication or authorisation:
   1) by means of the System – if in possession of a legacy authorisation phone
   2) by submitting an appropriate request on the website or at a bank branch – if he or she does not have an existing telephone number for authorisation.

Article 26

1. To ensure security, the mobile device intended for the use of all the functions of the mobile application must be added to the list of trusted mobile devices. Where a single mobile device has been indicated as trusted by several users, each of those users is obliged to comply with the security requirements defined in the General Terms and Conditions, including the safe termination of the use of the application.
2. A list of trusted mobile devices is available in the System.
3. The user can remove a mobile device from the list in the Internet Banking System or in the mobile application. The Bank has the right to remove a mobile device from the list when there is reasonable doubt that the user does not use the device or that an unauthorised person has gained access to the device. It is assumed that the user does not use a mobile device if he/she has not logged into the mobile app on that device for 90 days. The user can add the device to the list again. For security reasons, a device may also be removed from the list

automatically – depending on the version of the mobile application – as a result of activation of the application on another device.

4. A trusted browser can be removed from the list in the Internet Banking System. The Bank has the right to remove a trusted browser from the list when it has reasonable doubt that the user is not using the device or that an unauthorised person has gained access to the device. For security reasons, a trusted browser will be removed from the list after 90 days from the date it was added to the list of trusted browsers. The user can add the trusted browser to the list again.
5. Removal of a security key from the list of keys is possible in the Banking System when authentication with the security key has previously taken place or at a bank branch or the call centre.
6. In case of loss, theft, misappropriation or unauthorised use of a trusted mobile device, the user will remove the suspected device from the list in accordance with sec. 3 as soon as possible.
7. In the case of a suspicion of unauthorised use of the System or theft or misappropriation of the device to which the telephone for authorisations is linked, or suspicion of intentional causing of an unauthorised transaction, the user is obliged to notify the Bank immediately by means of the Internet Banking System or via the helpline.

Article 27

1. The Bank reserves the right to carry out upgrades, updates and regular technical maintenance of the Internet Banking System, which may result in periodic interruptions of access to the System or to its selected functionalities. The Bank will inform the user about the above circumstances, stating the estimated time of an access interruption or restriction:
   1) via the message option in the Internet Banking System, and/or
   2) on the Bank's website, and/or
   3) via the helpline.
2. The Bank reserves the right to block access to the Internet Banking System for security reasons. Security reasons are understood to mean situations or threats of unauthorised access by third parties to accounts, products or banking services through the System and in cases prescribed by law.
3. In the case of a suspected attempt at unauthorised access to the System, the Bank may suspend the possibility of logging on to the System for a specified period of time. The Bank will inform you of how to log back into the System in a message sent to your phone for authorisation.
4. The Bank reserves the right to refuse to carry out an instruction or to introduce additional restrictions and safeguards with respect to instructions given via the Internet Banking System, if there are important circumstances preventing the execution of such instructions, i.e. technological obstacles, security reasons or an instruction's content violating the Bank's regulations binding for the user, as well as in the case of the user's failure to comply with generally applicable provisions of law.
5. The Bank may impose restrictions on the use of the Internet Banking System in the event that, based on the location of the IP address, it determines that the user logs on to the system in a country that is on the list of high-risk countries. The list of such countries and the extent of the restrictions are detailed on the Bank's website.
6. The Bank reserves the right to limit functionalities available in the Internet Banking System with respect to a group of users of a certain legal of factual status. These restrictions may be due to safety requirements. The Bank will inform users of the restrictions introduced at least 14 calendar days prior to the date of their introduction.
7. For reasons of security, the Bank has the right to request up-to-date personal data from the user or to confirm these data.
8. The user is not allowed to input or upload illegal content into the System, or to use programs that threaten other users of the System or endanger the integrity of the System, including the data stored in the System or its applications. If a particular service of the System, including a mobile application, enables the display of other persons' data, the user is not entitled to collect such data and may use it only to order a transaction.
9. When using the System, the Bank may provide the user with instructions on the technical and organisational tools of the System or announcements about services or functionalities made available within the System. Instructions and announcements are for information purposes only and do not constitute advertising. They may be communicated using the means of communication available in the System or may be presented in a visual, textual, animated form or as a presentation, among others.

14. Technical requirements for use of the system

Article 28

1. The user is allowed to use the System after meeting the following minimum technical requirements: having an electronic device, in particular a computer, a mobile phone, another mobile device with Internet access, an operating system and an Internet browser installed on that device. If the user wishes to use functions supported by separate applications, e.g. a mobile application, it is necessary to install the respective application on the mobile device.
2. During the term of the Agreement, the user must designate a phone for authorisations and must be in possession of the last indicated phone. Failure to indicate a phone number for authorisations will prevent the user from using the System or its particular functions.
3. Technical requirements related to the communication between the user and the System:
   1) for Internet banking – operating system Apple OS X and Windows
   2) for the mobile application – iOS and Android operating systems.

   Additional information relating to the user's communication with the System or with specific applications, programs, file types or concerning Internet browsers and their versions and operating system versions is provided in the Announcement and on the Bank's website.
4. Due to technical and technological developments, particular versions of the System may be updated, improved, changed or replaced by new versions. Where technically feasible, updates or enhancements may be made during the operation of the System. In the event that any of the above operations requires a restart or installation, by the user, of a new version of the System, the Bank will inform the user of this by means of appropriate screens, notifications or messages.
5. The Bank may withdraw an older version of a System, replacing it with a newer version. In such a case, the user will be informed, in good time, of the expected date of the replacement of the older version with the newer one and of the necessary actions, if any, if the user would be required to take any action for technical reasons, in particular to download and install the new version or to perform those actions on a given type of device.

15. Termination, notice and expiry of the agreement

Article 29

1. The client is entitled to terminate the Agreement with immediate effect, without notice. An instruction to terminate the Agreement may be submitted in writing otherwise being invalid, or via the Internet Banking System, provided that the System enables such a method of submitting a termination statement.
2. The Bank has the right to terminate the Agreement concluded with the client upon two months' notice.
3. The Bank will have the right to terminate the Agreement concluded with the Client with an appropriate notice period, as indicated below, in the event of (valid reasons of termination):
   1) the Bank determining that the user does not comply with the Principles of the safe use of the system, as described in Chapter 13 of the General Terms and Conditions,
   2) the Bank obtaining information that gives rise to reasonable suspicion that an offence has been committed by the user, including an offence involving the Internet Banking System or an offence detrimental to the Bank,
   3) the user's failure to provide the information described in the General Terms and Conditions, necessary for the activation of a service or for the continued provision of the Internet Banking System service,
   4) the user's provision of data or information that is untrue or inaccurate, including the use of outdated documents (including documents past their validity date), as well as false, forged or counterfeit documents,
   5) the Bank's inability to fulfil its obligations in applying the financial security measures set out in the Act on the Prevention of Money Laundering and Terrorist Financing.
4. The agreement is terminated on the death of the client. The following are considered verifiable documents that

may be submitted to confirm the death of the client:

1) a full or abridged copy of the death certificate,

2) death certificate,

3) a letter from the pension authority;

4) information from the register of the Public Electronic System for Population Registration (PESEL);

5) a letter from the police, court, bailiff, and

6) another verifiable document confirming the client's death.

If a given document raises doubts, in particular, as to its authenticity or confirmation of the fact or date of the user's death, or if there are other important circumstances giving rise to doubts as to the fact or date of the user's death, a full or abridged copy of the death certificate will be considered by the Bank as the document confirming the fact of death, unless a court ruling or the law provides otherwise.

16. Complaints. Dispute resolution

Article 30

1. Complaints concerning payment orders envisaged in these General Terms and Conditions but related to accounts regulated in the General Terms and Conditions for Accounts for Retail Clients, are subject to the provisions of those General Terms and Conditions that are applicable to a given account. The authority to conditionally credit or debit the account with amounts resulting from a complaint, which is granted by the user in accordance with the account agreement, will also cover transactions resulting from payment orders under these General Terms and Conditions. Supporting information on accounts that are subject to the General Terms and Conditions for Accounts for Retails Clients.

2. Complaints regarding unauthorised, incorrectly initiated or improperly executed or non-executed instructions that have been submitted via the System must be made without delay, however not later than within 13 months of the date of the questioned instruction.

3. Subject to the provisions of Article 22 and Article 22a, in the case a payment transaction unauthorised by the person entitled to dispose of the account is executed on the account, the Bank will return immediately – however not later than by the end of the business day following the day on which it was ascertained that the payer's account has been debited with an unauthorised transaction, or following the day on which the Bank received the relevant notification, except where the payer's provider has reasonable and duly documented grounds to suspect fraud and reports this fact in writing to law enforcement authorities – the amount of the unauthorised payment transaction and restores the debited account to the state it would have been in had the unauthorised payment transaction not occurred.

4. The user has the right to lodge a complaint. A complaint can be made:

1) in electronic form:

a) via the Internet Banking System,

b) to the electronic delivery address entered in the electronic address database, which you can find on our website;

2) orally:

a) by telephone at the numbers indicated on the Bank's website (call cost at operator rates),

b) in person, at a bank outlet providing this service;

3) in writing:

a) by post, to the Bank's address indicated on the Bank's website,

b) in person, at a bank outlet providing this service.

5. In justified cases, complaints made via the Internet Banking System or by telephone via the call centre regarding unauthorised, incorrectly initiated, non-executed or inadequately executed payment transactions or instructions will be additionally confirmed by the user in writing at the bank branch carrying out this activity, within 14 calendar days from the date of submitting the complaint.

6. The Bank shall provide a response to the complaint on a durable medium using the same channel (except for verbal complaints) through which the user submitted the complaint, unless the user informs us that they wish to

receive it through a different channel.

7. The Bank will respond as soon as possible, but no later than 15 business days (for complaints relating to payment services) and 30 days (for complaints not relating to payment services) from the date of receipt. In the course of investigating a complaint, the Bank may ask for additional information or documents. In particularly complicated cases, which make it impossible to handle the complaint and provide a response within this period, the period may be extended, but may not exceed 35 business days (for complaints relating to payment services) and 60 days (for complaints not relating to payment services), counting from the date of receipt of the complaint. The Bank will inform the user of the reasons for the delay, indicate the circumstances that need to be established in order to consider the complaint, the expected date for the completion of the complaint procedure.
8. During the complaint procedure the Bank may ask the user to provide additional explanations or documents. If it is necessary to clarify additional circumstances in connection with the complaint procedure, the Bank reserves the right to contact the user by telephone at the telephone number indicated by the user for contacting the Bank.
9. If a complaint is not accepted by the Bank, the user has the right to appeal. Insofar as the user is aware of new relevant facts, circumstances or evidence, he/she will disclose them to the Bank in the request. The Bank will re-examine the complaint within the time limits specified for the examination of complaints.
   If a dispute arises between the client and the Bank as a result of a complaint, it may be resolved amicably through a settlement agreement.
10. Any disputes that arise from the agreement concluded by the Bank and the user may be settled out of court. Requests can be submitted to:
    1) Financial Ombudsman, website: www.rf.gov.pl. The Ombudsman acts in accordance with the Act on Complaints Handling by Financial Market Operators and the Financial Ombudsman and on the Financial Education Fund;
    2) The Bank Arbitrator operating at the Polish Bank Association, website: www.zbp.pl/dla-konsumentow/arbiter--bankowy/dzialalnosc. The Arbitrator will resolve the dispute and issue his/her award in accordance with the general terms and conditions of the Banking Consumer Arbitration.
11. The user may also turn to a consumer ombudsman (municipal or district) for assistance.
12. Disputes arising from the Agreement may also be resolved in court. The court competent for resolving disputes will be determined in accordance with the provisions of the Code of Civil Procedure.
13. An user may file a complaint with the body that supervises the Bank (Polish Financial Supervision Authority) against the Bank's action if, in the user's opinion, this action breaches the provisions of law and in the case of a refusal to provide payment services to the user.

17. Amendment of the General Terms and Conditions

Article 31

1. The Bank reserves the right to amend the General Terms and Conditions for valid reasons. The following reasons will be deemed to be valid and requiring amendment of the General Terms and Conditions to the extent necessary for that reason:
   1) the introduction of new or amended legislation which sets out the rules of the provision of services by the Bank or which sets out the rules of the use of such services by the user,
   2) issuance by a supervision authority or any other authorised entity of a decision, recommendation, recommendation, position, ruling or any other document specifying the rules of the provision of services by the Bank, or specifying the rules of the use of such services by a user under an agreement concluded with it,
   3) extension, change or limitation of the functionality of the services, change of the rules of using the services by the user, introduction of new services, abandonment of certain activities being the subject of the services provided by the Bank under the agreement concluded with the user
   4) changes to the Bank's IT system resulting from:
      a) improvements to the Bank's IT systems due to technological developments,
      b) mandatory changes made to interbank settlement systems in respect of participants of those systems,

c) changes of software suppliers resulting in changes in the functionality of the Bank's IT system,

– affecting the services covered by these General Terms and Conditions provided by the Bank or the rules of use of such services by the user under the agreement concluded with him/her.

2. The Bank will notify the user of amendments to the General Terms and Conditions in the manner agreed with the user and set out in Article 32 sec. 2 no later than two months before the proposed effective date of the amendments to the General Terms and Conditions.
3. The user will have the right, prior to the date of the proposed entry into force of the amendments:
   1) terminate the Agreement without charge with effect from the date on which he/she is notified of the amendments but no later than the date on which the amendments become applicable,
   2) object to the proposed changes.

   If the user does not object to the changes in writing prior to the proposed effective date, he/she will be deemed to have agreed to them. In the event that the user objects but does not terminate the Agreement, the Agreement will terminate on the day prior to the effective date of the proposed changes, without charge.
4. The change of functionalities of the System or individual services, which is caused by technical/technological development, does not necessitate the amendment of the General Terms and Conditions as long as it does not change the principles of the services provided to the user under the Agreement concluded with him/her.
5. Prior to the proposed effective date of changes to the General Terms and Conditions, the Bank may allow the user to use changes to existing services or to use new services, provided that the user accepts the change to the General Terms and Conditions relating to the service in question.

18. Final Provisions

Article 32

1. The General Terms and Conditions are available at bank outlets and on the Bank's website.
2. The Bank will notify the client of any changes of the General Terms and Conditions by sending a notification on a durable medium:
   1) via the Internet Banking System, or
   2) in any other manner agreed by the parties.
3. Chapter titles are provided for information purposes only, to facilitate understanding of the text of the General Terms and Conditions.
4. The General Terms and Conditions are valid from 22 March 2026.

Appendix 1

Manner of execution of payment orders and other instructions submitted via the internet banking system

The cut-off times for accepting payment orders through the Internet Banking System depend on the hours of operation of the Bank's systems, as shown in the table below. A payment order submitted via the Internet Banking System after a cut-off time shall be deemed to have been received on the first business day following the day on which the order was submitted.

Manner of execution of payment orders for credit transfers, standing payment orders:

Cut-off time for receipt of payment orders	**Type of payment order**	
	With current execution date	**With deferred execution date** regardless of the time of placing the order
	Orders that do not require currency conversion	
none	a) internal transfer order in PLN or transfer within the "Pay with ING" service	
order executed in real time	b) internal transfer order in foreign currencies, c) domestic transfer submitted as Express ELIXIR or BlueCash transfer	a) internal transfer order in PLN b) internal transfer order in foreign currencies c) standing orders to accounts in the bank
none order executed according	Orders that do not require currency conversion	
to the Bank's schedule of settlement sessions	a) a domestic transfer, including one made as a transfer within the "Pay with ING" service	a) domestic transfer b) standing orders to accounts in other banks
3.00 pm (Monday to Friday)	Orders that do and do not require currency conversion	
	a) TARGET transfer	a) TARGET transfer
5.00 pm (Monday to Friday)	Orders that do not require currency conversion	
	a) foreign currency transfer abroad b) SEPA credit transfer c) foreign currency transfer order	a) foreign currency transfer abroad b) SEPA credit transfer c) foreign currency transfer order
	Orders that require currency conversion	
	a) domestic transfer b) foreign currency transfer abroad c) SEPA credit transfer d) foreign currency transfer order	a) domestic transfer b) foreign currency transfer abroad c) SEPA credit transfer d) foreign currency transfer order
7.00 pm (Monday to Friday)	Orders that require currency conversion	
	a) internal transfer order in PLN b) internal transfer order in foreign currencies	a) internal transfer order in PLN b) internal transfer order in foreign currencies

Cancelling transfers made via the internet banking system

Type of transfer that can be cancelled – with current execution date	When a transfer can be cancelled
User may cancel in the Internet Banking System a transfer from savings and settlement accounts submitted via this System, with the exception of transfers with a current execution date initiated by the provider of a payment transaction initiating service	
• a domestic transfer that does not require currency conversion and is not executed in real time and is not submitted as a transfer within the "Pay with ING" service	• submitted **between 00.01 am and 8.15 am Monday to Friday** may be cancelled until 9.00 am on the day of submission • submitted **between 8.16 am and 11.35 am Monday to Friday** may be cancelled until 1.00 pm on the day of submission • submitted **between 11.36 am and 2.45 pm Monday to Friday** may be cancelled until 3.30 pm on the day of submission • submitted **between 2.46 pm and 12.00 pm Monday to Friday** may be cancelled until 9.00 pm on the next working day • submitted **between 00.01 am and 12.00 pm Saturday, Sunday or Bank holiday** may be cancelled until 9.00 am on the next business day
• TARGET transfer • domestic transfer which requires currency conversion • foreign currency transfer abroad • SEPA credit transfer • foreign currency transfer order	• submitted **between 5.01 pm and 12.00 pm Monday to Friday** can be cancelled until the start of the next working day (until 00.00 am) • submitted **from 00.01 am Saturday, Sunday or Bank holiday** may be cancelled until the start of the next business day (until 00.00 am)
• an internal transfer order which requires currency conversion	• submitted **between 7.01 pm and 12.00 pm Monday to Friday** can be cancelled until the start of the next working day (until 00.00 am) • submitted **from 00.01 am on a Saturday, Sunday or Bank holiday** may be cancelled until the start of the next business day (until 00.00 am)

We will return the money for the cancelled transfer to your account on the next working day at the latest.