EUROBANK
Private Bank Luxembourg

EUROBANK PRIVATE BANK
LUXEMBOURG S.A.
534, rue de Neudorf, L-2220 Luxembourg

eurobankpb.lu

RC. B24724

Use of Eurobank Private Bank Luxembourg S.A. E-Banking Service Specific Conditions

July 2021

1. General Information

The present Specific Conditions govern the rights and obligations of Eurobank Private Bank Luxembourg S.A and the undersigned (hereafter referred to as the "**Client/User**" with individual signature power either as account holder, representative or attorney) to access one or more of their Accounts held with the Bank, through the use of the E-Banking Service available on the Bank's Website.

2. Definitions

- "**Account**" means all accounts and the data related to such accounts accessible by the Client/User through the E-Banking Service, as agreed between the Client and the Bank.
- "**Bank**" means Eurobank Private Bank Luxembourg S.A., a public limited company (Société Anonyme) subject to Luxembourg law, registered under n° B24724, with its registered office in 534 rue de Neudorf, L-2220 Luxembourg, authorised in the Grand Duchy of Luxembourg as a credit institution and subject to prudential supervision by the financial supervisory authority in Luxembourg, the Commission de Surveillance du Secteur Financier (the "CSSF").
- "**Client**" means the physical person or the corporate entity, maintaining a business relationship with the Bank as account holder.
- "**Device**" means a Personal computer (PC), a mobile phone, a tablet or any other similar device allowing access to Internet.
- "**E-Banking Service**" or "**E-Banking**" means the electronic banking service available on the Website managed by the Bank and provided via Internet.
- "**Incident**" means the loss or theft of the personal authentication elements, the disclosure to a third party (even if involuntary or merely suspected) of any access codes, misappropriation or any other unauthorised use of the personal authentication elements by the Client/User or by a third party as well as the loss, theft, or disclosure to a third party (even if involuntary or merely suspected), misappropriation or any other unauthorised use of the personalised security features of the Client/User.
- "**Spending limits**" means the spending cap or maximum number of authorized payment orders, as agreed on by the Bank and the Client for each payment instrument.
- "**User**" or "**Users**" means the appointed individual(s) authorised by the Client to access the Account through the use of the E-Banking Service or the Client himself.
- "**Website**" means the public corporate website of the Bank, accessible under https://www.eurobankpb.lu/.

3. Services

Without prejudice to any future amendment(s), the services available to the Client/User through E-Banking include but are not limited to the following:

a) Portfolio Overview
   - Presentation of the Account portfolios, balances and transactions.
   - Presentation, generation and printing of Account statements, and Advices with details of the corresponding transactions.

b) Payment Services

- Submission of single fund transfers, multiple fund transfers, e.g. hub payments, salary payments, etc. (hereafter referred to as "payment orders") or standing orders.
- Registration of Beneficiaries.

c) Secure Messaging
- Accessing a secure electronic messaging service, which permits the exchange of confidential information with the Bank.

Any service that is not governed by the present Specific Conditions is governed by the General Terms and Conditions and the Bank's Specific Conditions - Payment Services.

3.1. E-Banking Portfolio Overview Service

The E-Banking Service enables the Client/User to select a given Account and to obtain the relevant statement for a selected period. Such statement will then be made available to the Client/User on the E-Banking platform. In any case, the Bank will notify the Client/User of any new document made available through the mean of communication agreed between the Bank and the Client.

If the Client/User has opted to consult his/her Account and related correspondence solely via the E-Banking Service, the Client/User shall undertake to read and consult them at regular intervals. Transmission of the Bank's correspondence by normal post shall consequently be discontinued, unless specifically requested by the Client.

At the discretion of the Bank or in case of technical issues, which render the E-Banking Service inaccessible, the Bank shall also be entitled to deliver documents in hard copies by normal post or by other means of communication agreed between the Bank and the Client.

Electronic bank documents, including statements, shall be deemed to have been duly provided on the day on which they are made available on the E-Banking. All relevant time limits (including in particular the time limit for complaints) shall begin to run on this day.

By using the E-Banking Service, financial data and market data provided by third parties can be consulted for information purposes only and should not be considered as an advice from the Bank. All data is collected from reliable sources and is transmitted to the Client/User in non-real time mode. Under no circumstances, the Bank shall be held responsible for any error or failure related to the reliability, integrity, accuracy or the content of the information provided by third parties as well as for any direct and/or indirect damage resulting from the use made by the Client/User of the information provided by third parties.

3.2. E-Banking Payment Services

Payment Services are also governed by the Bank's Specific Conditions – Payment Services.

Payment orders can only be executed by the Bank if the Client/User authorizes them through the Secure App (please refer to section 5.4 for details on the Secure App).

The Client/User has the obligation to submit the payment orders in accordance with the present Specific Conditions. In case the Bank refuses to execute an order, the Client/User will be notified accordingly and, unless prohibited by relevant national or European or international legislation, will be informed about the grounds for such refusal and the procedure to correct any factual error that led to the refusal at the earliest opportunity.

Payment orders submitted via E-Banking may only be revoked within the time limit allowed by the E-Banking

service (i.e. prior to execution), otherwise only if they are technically and procedurally reversible by the Bank. In this case, the Client/User is liable for possible revocation expenses either of the Bank, according to the Bank's Pricing for Services and Financial instruments (hereafter referred to as "**fee schedule**") of fees or of third parties, in force at that time.

The Bank reserves the right not to execute specific payment orders, or to temporarily suspend the possibility of submitting orders via E-Banking for reasons relating to maintenance and upgrading of its technological infrastructure, security reasons and any other justified reasons, including but not limited to the suspicion of unauthorised or fraudulent use of a payment instrument, insufficient credit balance of the Client/User to validly fulfil payment orders as well as the security of the Client/User and of the Bank itself. The Bank will inform the Client/User of such circumstances by any means the Bank will deem appropriate, if applicable before denying executing a payment order or at the latest immediately afterwards, unless giving such information would compromise objectively justified security reasons or is prohibited by relevant national, European or international legislation.

The temporary suspension by the Bank of the Client/User's right to submit payment orders via E-Banking may take place at any time, if deemed necessary by the Bank, without having an obligation to disclose to the Client/User the reason for the suspension. The Bank has, however, an obligation to notify the Client/User of the fact that transaction suspension is applied.

Spending limits apply for payment orders via E-Banking. Spending limits for each authorised User are requested by the Client and are imposed into the E-Banking Service. The Bank reserves the right to decrease the applicable spending limits if deemed necessary.

Payment orders received by the Bank via E-Banking after the cut-off times, as defined per currency within the Bank's fee schedule, or outside of business hours will be executed on the following business day.

Some transactions are not automatically processed or immediately transmitted to the various intermediaries for execution. The Client/User may use the E-Banking Service 24 hours a day. However, the execution of payment orders shall also depend on the business hours of the correspondent institutions and systems involved, such as settlement systems and clearing houses.

The Bank reserves the right to ask the Client/User to provide any supporting documentation required (contracts, invoices etc.) for the proper execution of a payment order.

3.3. E-Banking Secure Messaging Service

The E-Banking Secure Messaging Service enables the Client/User to send information, documents and messages to the Bank through a secured messaging module.

Messages sent to the Bank via Secure Messaging must not include payment orders, blocking instructions (e.g. blocking User access to the E-Banking or blocking Credit cards) or any other instruction subject to execution within a specific time limit. Any damage incurred by the Client/User as a result of notifications in breach of this provision shall be borne solely by the Client.

Unless otherwise agreed between the Bank and the Client, mandatory information required by any applicable law to be provided to the Client/User will be provided through the E-Banking Secure Messaging. In this context, the Client/User undertakes to connect regularly to the E-Banking in order to receive all information that may be of interest or use to him/her.

Once the Bank receives a secure message – and subject to other conditions stated herein – the Bank will

contact the Client/User to address the expressed need through the same mean of communication within a reasonable period. If the Bank deems necessary, alternate communication might be utilized as well (e.g. email, phone call).

Notwithstanding the above, the Bank may at its discretion request from the client to verify an instruction using the secure messaging functionality of the e-Banking service, or confirm the instruction with the client through any other means in line with the procedures of the Bank.

Any communication shall be made in English.

4. E-Banking Access

Access to E-Banking is subject to prior acceptance by the Bank.

The Bank reserves the right to either accept or reject a request to access the E-Banking Service on the basis of a duly signed and completed E-Banking Application Form and/or any other document required by the Bank from time to time in relation to the E-Banking Service.

Only physical persons identified as "**Client/User**" are authorised to access the Bank's E-Banking Service. In this context, the Bank shall deem the use of any service, including but not limited to the submission of instructions, payment orders or secure messages by a User as submitted by the Client.

Access to E-Banking Service is available through the dedicated link provided on the Bank's Website.

5. Personal Authentication Elements

Due to enhanced security requirements introduced by the Revised Payment Services Directive (EU) 2015/2366 (hereafter referred to as "**PSD2**"), the Bank applies the principle of Strong Customer Authentication (hereafter referred to as "**SCA**") to ensure confidentiality of the personal and financial data of its Clients.

To this respect, the Client/User will receive the following unique personal authentication elements:

- One username (the "**Username**"),
- One initial password (the "**Password**"),
- One technology based hardware security element (a small card-sized device hereafter referred to as "**Token**"), generating one-time-passwords (the "**OTP**") and
- One technology based software security element for the authorization of payment orders, registration of beneficiaries and other actions if imposed by the bank (the Eurobank Lux Secure App, hereafter referred to as "**Secure App**").

The Bank will send the Username and the Token to the Client/User via normal mail to the address indicated in the respective E-Banking Application Form

The Bank will send the initial Password to the Client/User via SMS to the mobile phone number indicated within the respective E-Banking Application Form.

The Secure App is available on the "Apple Store" and the "Google Play Store" and has to be downloaded by

the Client/User on his/her personal mobile phone.

The mobile phone has to be enrolled in the Bank's systems following the procedure described on the dedicated "Device enrolment" page of the E-Banking.

Each of the above personal authentication elements is strictly personal, and provided solely to the individual being granted access to the E-Banking Service.

5.1. Username

The Username is the security element uniquely identifying the Client/User. It is strictly personal to the Client/User and must neither be disclosed nor transferred to any third parties; it remains the property of the Bank, in addition to the initial Password and the Token.

5.2. Password

The initial Password supplements the above-mentioned Username and is required for the very first access of the Client/User to the E-Banking Service.

For security reasons, the initial Password must be modified during the first use of the E-Banking Service; to this respect the Client/User will be requested to change the initial Password to - a new Password of his/her preference which must neither be disclosed nor transferred to any third parties including the Bank and its Officers.

Under no circumstances, the Bank, its officers or any third party, will request the password of the Client/User.

The Bank may, at its discretion, impose an expiry date for the Passwords beyond which the Client/User will not be able to access the E-Banking Service without a prior modification of his/her Password. The Bank also reserves the right to reset the Client/User's Password, whenever this is deemed necessary.

It is highly recommended that the Client/User periodically changes his/her Password ensuring that it does not consist of easily identifiable combinations (such as his/her identifier, last name, first name or date of birth or those of someone close (spouse, child, etc..) and more generally a word or combination of words, a word spelled backwards, a word followed by a digit or a year, a password used for other purposes (including for personal e-mail, etc.).

The Client/User shall in particular choose to use a Password of sufficient length and composed, whenever possible, of a combination of letters, numbers and punctuation marks or special characters, as well as using uppercase and lowercase characters.

The Client/User must ensure that the E-Banking Service Password is not used for accessing other internet services.

In case of failure of the Client/User to access the E-Banking Service using his/her current password, the Client/User should contact the Bank requesting a password reset. In that case, the Bank will send a new "Initial password" to the Client/User via SMS to the mobile phone number indicated within the respective E-Banking Application Form.

5.3. Token

The Token is a hardware security element connected to the above-mentioned Username; its aim is to provide enhanced protection for the access to account information in accordance with the security principle of SCA.

By design, the Token displays an OTP with two primary characteristics: (1) the OTP has a short validity period of 30 seconds, and (2) each unique code may only be used once.

Once a code has been used already, or when its time-bound validity has expired, a new OTP must be used by the Client/User.

The Token is also strictly personal to the Client/User and must not be transferred to any third parties. The Bank reserves the right to recall or change the Client's Token whenever this is deemed necessary. The Client/User must ensure that his E-Banking Token is always stored at a safe place and cannot be accessed temporarily or permanently by any third party.

The Token is a hardware device assisting Client/User authentication. This personal authentication technology may also be used as part of other Bank services for the purpose of authenticating the Client/User or approving a payment order submitted by the Client/User.

5.4. Secure App

The Secure App is a software security element connected to the above-mentioned Username. The aim is to provide enhanced protection for the submission of payment orders, registration of Beneficiaries as well as any other action performed through a remote channel, which might imply a risk of payment fraud, in accordance to the security principle of SCA.

5.5. Obligations of the Client/User for the Protection of the Personal Authentication Elements

The Client/User is responsible for the protection of these elements against misuse and disclosure.

Access to the E-Banking Service shall never be shared, and no circumstances shall ever make such an arrangement acceptable.

The Bank reserves the right to modify the authentication process and/or elements as described above, in order to comply with national, European or international legislation and to protect the interests of the Client/User. In that case, a notification will be sent by the Bank via secure messaging, simple email or by any other means of communication agreed between the Client and the Bank.

The consecutive wrongful use of Client/User's personal authentication elements will result in the automatic blocking of the Client/User's access to the E-Banking Service. The Client/User may contact the Bank to ask for access, unblocking or the issuance of new personal authentication elements.

The Client/User hereby undertakes to use his/her best endeavours to preserve the confidentiality of the personal authentication elements, which allow access to the E-Banking Service and in particular:

- Not to write down his/her personal authentication elements anywhere, even in a coded form;
- To always use his/her personal authentication elements away from prying eyes and ears of others;
- To never let himself/herself be distracted while connected to the E-Banking, including by persons offering their help, and to ensure that he/she does not enter his/her personal authentication elements in the presence of others;
- To regularly consult his/her accounts to assess them for any Incident;

- To ensure that the Device used to access the E-Banking Service meets the minimum security criteria (use of updated antivirus programs, timely installation of software updates, no use of outdated/unsupported software and Devices, avoidance of non-authorised apps, websites etc. on Devices used to access the E-Banking).

The Client acknowledges that the Users have been informed of the content of the present Specific Conditions, of which they have received a copy, and that the Users have carefully reviewed them, understood them, accepted to abide by them and have undertaken to comply with such conditions. As a consequence, all obligations incumbent upon the Client regarding E-Banking Service security, access to the E-Banking Service and use of the E-Banking Service must also be complied with by the Users.

6. Client/User Authentication and consent

The Bank elects that the combined use of personal authentication elements is considered as indisputable proof of the Client/User's identity as well as evidence that all instructions originate exclusively from the Client/User. In this case, the Client/User authorises the Bank to proceed to the immediate execution of the submitted instructions, in the framework of and according to the terms of the present Specific Conditions.

The Client and the Bank expressly agree that the personal authentication elements as defined in section 5 shall have the same value in evidence as the original signature of the Client/User.

7. Technical equipment and secure use of the Internet

7.1. IT equipment and requirements

The Internet is an international network of telecommunications to which the Client/User may have access through any suitable Device. To access the E-Banking Service of the Bank via the Internet, the Client/User must comply with the technical requirements (regarding hardware and software) as described in the Bank's Website.

The Client/User shall take all necessary measures to ensure that the technical characteristics of his/her Device, software and Internet connection allow him/her to access the Bank's Website and the E-Banking Service in a secured manner. In particular, the Client/User has an obligation to have installed on his/her Device the latest and updated editions of programs, operating systems and versions of antivirus programs and relevant programs of protection of data and Devices (antispyware, firewalls, etc.), to ensure that they are in compliance with the Bank's systems and under no circumstances to store on the Device non-recognised programs or programs without a legal permit for the installation in question.

The Client/User is fully liable for the proper functioning of his/her own Devices and shall ensure that such Devices do not have any apparent problems or viruses and provide sufficient security to prevent a risk of any third party access to data pertaining the E-Banking Service.

The Client/User will use his/her best endeavours to maintain such security and shall further ensure that there is no risk of any hostile programs or viruses invading and disrupting the IT systems which are used to provide the E-Banking Service. In particular, the Client/User will ensure that the security of his/her Device is sufficient and will regularly update the antivirus and antispyware software as well as his/her personal firewall.

The Client/User shall bear all technical risks such as the disruption of electric power transmission, non-availability of communication lines, improper functioning or overloading of the systems or networks.

7.2. Secure use

The Client/User shall be liable for the proper use of the E-Banking Service in accordance with the technical

requirements, security instructions and any other instructions provided by the Bank through its Website or through any other means of communication agreed between the Client and the Bank.

The Client/User undertakes to comply with all security instructions provided by the Bank.

Under normal circumstances, the E-Banking Service shall be accessed via the Bank's Website, or (if applicable), the dedicated link communicated by the Bank directly to the Client/User, except in case of unavailability (*e.g.* in case of maintenance). In order to reduce the risk of unauthorised access by third parties to the E-Banking Service, the Client/User should only directly connect to the Bank's Website and not indirectly, *e.g.* through shared or stored links. Any indirect access by the Client/User to the Bank's Website is done at the sole risk of the Client/User.

The Client/User shall be connected to the Bank's Website for the use of the E-Banking Service for a limited period of time and shall log off as soon as he/she has completed his/her operations. In this context, the Client/User understands that once logged in, he/she remains connected to the E-Banking Service until he/she proceeds to the log off by clicking on the log off section of the E-Banking. An automated log off has been set after a certain period of inactivity.

7.3. Access via Internet

The Client/User confirms that he/she is familiar with the Internet and that he/she is aware of the technical characteristics thereof, including the related technical performances and response time for downloading or transferring information on the Internet.

Furthermore, the Client/User is aware that he/she will be required to subscribe to an Internet Service Provider ("**ISP**") of his/her choice in order to gain access to the E-Banking Service. In this context, the Client/User hereby agrees and understands that he/she is liable for the selection of the ISP and for the set-up of the terms and conditions of their relationship. The Bank will not be held liable for the risks created by the access to the Internet and by the transmission of data from or to the Client/User, in particular in case of conflict between the Client/User and the ISP in relation to the personal and/or confidential nature of the Client's data, the cost of the transmission, the maintenance of the telephone lines and of the Internet structures or the interruption of services.

Access to the E-Banking Service via the Internet is protected by a multi-level security system. For example, the Client/User may not access the E-Banking Service without identifying himself/herself.

7.4. Security on the Internet

In the development of the E-Banking Service and its functionalities, special emphasis has been placed by the Bank on security. To protect the Client/User, a multi-level security system has been developed, which, among other things, makes use of high-standard encryption processes. In principle, this encryption makes it impossible for unauthorised persons to gain access to the Client/User's confidential data and personal authentication elements. However, despite the use of state-of-the-art security mechanisms and the development of secure software, absolute security cannot be guaranteed on neither the Bank's side nor the Client/User's side. The Client/User duly notes that his/her own Device can be a particularly weak point in terms of E-Banking security.

The Client/User duly notes the following risks in particular:

- The Bank cannot guarantee either unlimited access to the relevant services or unlimited use of the same. Nor can the Bank guarantee the unrestricted operational availability of the Internet.
- Inadequate knowledge of the system and faulty security precautions on the Client/User's Device (e.g. inadequately protected storage of data on the hard disk, file transfers, unauthorised „screen

peeking") may facilitate unauthorised access. It is the Client/User's responsibility to ascertain exactly what security precautions are required and to comply with them.

- While the communication from the web browser to the E-Banking Service is encrypted with the highest available standards, by drawing up an Internet traffic profile, the Client/User's Internet provider is able to determine with whom the Client/User has been in contact and when such contacts took place.
- There is a latent danger that, when the Internet is being used, a third party could gain access to the Client/User's Device without being noticed (e.g. by means of a Trojan horse, virus, etc.).
- In spite of security measures, when using the Internet, there is a constant danger of computer viruses spreading to the Client/User's Device as soon as it comes into contact with the outside world. Anti-virus scanners can assist the Client/User in protecting his/her system and are urgently recommended.

Moreover, it is important to stress the importance of using only software from trustworthy sources, and to maintain them up-to-date to minimize the risk of potential software vulnerabilities.

8. Type of Accounts legitimate for E-Banking access

8.1. Individual and/or joint accounts (accounts of natural persons)

In case of Individual Accounts and further to the approval by the Bank of the E-Banking Application Forms duly completed and signed by the Client/User, the Client/User will receive a single set of Username, initial Password and Token providing access to the account(s) as listed in the E-Banking Application Form.

In case of joint accounts and if the appointed User(s) is/are the account holder(s), the Bank may receive an E-Banking Application Form duly completed and signed by the account holder(s) who will be the User(s).

Subject to the conditions mentioned above, the instruction will be deemed as validly given by all the account holders.

In case of joint accounts and if the appointed User is not one of the account holders (e.g. an attorney), the Bank shall receive an E-Banking Application Form signed by all the account holders of the account(s).

Whenever the Client appoints one or more agents or attorneys as User(s), each agent or attorney will receive his/her own personal authentication elements referred to under section 5. In the case of joint Accounts, each person having authority and power to access and/or operate the Account through the E-Banking, must validly execute and comply with the present Specific Conditions. The same shall apply to any agent or attorney having power and authority to operate the Account.

All persons having power and authority to operate a joint Account shall be jointly liable towards the Bank, together with their respective agent(s), without prejudice to the legal provisions applicable to agency agreements.

8.2. Corporate Accounts

E-Banking access to corporate (legal persons/entities) accounts is feasible through the appointment of designated individual(s) authorised by the Client to access the Account through the use of the E-Banking Service (the "Users").

The authorized signatories of the Account or the persons appointed by the Board of Directors or the Board of Managers, depending of the legal from of the corporate entity, select such Users through specific resolutions adopted to that effect.

8.3. Blocking and Revocation of a User's access rights

The Users and their access rights in respect of the E-Banking Service shall not cease for any reason (*e.g.* in case of a later change of the composition of the board of directors or later election of a new board of directors or later removal of the authorised signatory for any reason whatsoever, termination of an agency agreement or revocation of a Power of Attorney), for as long as a formal revocation of a User has not been duly notified in writing to the Bank by the Client.

Such revocation or termination of the authority given by the Client to one or more agents/attorneys as Users to act in relation to the E-Banking Service shall only become effective on the business day following the day of receipt by the Bank of a written instruction of the Client requesting the removal of the relevant User. This means that the Bank will continue to rely for any matter relating to the E-Banking Service and the appointed Users on the authorization in place until it has received a written notice that the powers of a specific User have been revoked by the Client.

The Bank cannot be held responsible for any actions, damages, loss and claims carried out, sustained or suffered by the Client as a result of the transactions initiated by a User that has been revoked by the Client for as long as the Bank has not been informed in accordance with the above mentioned procedure.

The Client can request the Bank by the most appropriate means of communication to block the access of a User even prior to the receipt the written revocation instructions mentioned above.

In that case, the Bank will block the access of the Revoked User on the same business day while the revocation will take place in accordance with the above mentioned procedure.

9. Liability of the Client/User

The Client/User recognises that the Bank has no responsibility for the actual or consequential damage which he/she is likely to sustain from his/her failing to fulfil his/her obligations which derive as a whole from these Specific Conditions, specifically from this section as well as the conditions provided within the Bank's Specific Conditions – Payment Services.

The Client/User is responsible for any damage sustained by the Bank owed to actions or omissions of the Users as well as to any illegal, anti-contractual or/and questionable action by them or by the Client himself/herself.

The Client/User has full responsibility for the carrying out of any payment orders by a third party until the moment the Client has duly notified the Bank about the leaking of the personal authentication elements.

The Client shall be responsible for any damages that he/she may suffer due to his/her failure to comply with his/her undertakings set out herein and, in particular the disclosure of his/her personal authentication elements because of him/her failing to comply with his/her obligations in particular when an Incident occurs. If an Incident occurs, the Client shall bear any costs for replacement thereof.

If an Incident occurs, the Client/User shall immediately inform the Bank. The Client/User shall then immediately request new personal authentication elements. The above shall also be applied in case the Client/User does not remember one or several element(s) of his/her personal authentication elements. In addition, it is also recommended that the Client/User modifies, without delay its Password.

In case the Client/User notes or suspects an abuse or a risk of abuse of the E-Banking Service, or in case he/she has lost his/her personal authentication elements, or suspects that a third party has or might have obtained his/her personal authentication elements by theft or otherwise or he/she has not received his/her personal

authentication elements within a reasonable time, he/she shall immediately notify the Bank via any of the agreed means of communication. The Client/User shall not bear any financial consequences after he/she has duly notified the Bank, except where the Client/User himself/herself has acted fraudulently.

Given that the provision of financial services from a distance and the encryption of communications via electronic networks is regulated in a different way from one country to another, the Client/User has an obligation to be informed and to abide by the law which regulates the provision of financial services from a distance and the encryption of communications via electronic networks, in the country in which he/she is registered.

The Client/User commits to regularly check his/her statements and the situation as regards the execution of his/her/its instructions, to inform the Bank immediately of any anomaly.

The Client/User commits to logging off from the E-Banking service when he/she is no longer using this service, even temporarily.

The Client/User acknowledges and accepts that if payment orders are submitted through the use of his/her personal authentication elements, the Bank is not obliged to perform any additional identity verifications.

The Bank reserves the right to block, temporarily or permanently, without prior notice, access to the E-Banking Service for duly justified reasons or in the event of a serious breach of the Client/User's contractual obligations.

10. Liability of the Bank

The liabilities of the Bank derive from this section as well as the Bank's General Terms and Conditions as well as the Bank's Specific Conditions – Payment Services.

Under normal circumstances, the E-Banking Service shall be available at any time on a 24/7 basis.

Nonetheless, access to the E-Banking Service is subject to the availability and operating capacity of the Bank's technical infrastructure and may be temporarily reduced or suspended for regular and/or required maintenance to remediate operational issues of the system or may be unavailable due to circumstances beyond the Bank's control, such ('***Force Majeure* events'**).

Under the present Specific Conditions, the following events shall be considered as "***Force Majeure* events**": Civil or military action, acts of terrorism, war, riot, explosion, sabotage, insurrection or revolution, requisition, acts of God, total or partial strikes inside or outside the premises belonging to the Parties, lock-outs, epidemics, blockage of transport or power supply for any reason whatsoever, adverse weather conditions, earthquakes, fire, storms, floods, water damage, government or statutory restrictions, governmental action (including any action taken by a court, tribunal, central bank), blocking or unavailability of communication systems (particularly telecom networks and Internet), systems' breakdowns, hacking of or any other type of attack against systems, embargo, investment or currency exchange restrictions, blocking or freezing of transactions by any sub-custodian, securities settlement system or other intermediary, changes to commercial legislation, etc.

Any of the above circumstances entitle the Bank to interrupt the provision of the E-Banking Service until further notice. The Bank shall not be liable for any loss or damage suffered by the Client/User as a result of the non-availability of the E-Banking Service due to the aforementioned events.

The Bank reserves the right to withdraw the access to the E-Banking Service if it reasonably suspects that the

access might be unlawful or might be associated with financial crime/fraud or if it reasonably believes that by accessing the E-Banking Service it might breach its compliance obligations. In this situation, the Bank shall not be liable for any loss or damage suffered by the Client/User as a result of the non-availability of the E-Banking, except in case of gross negligence or wilful misconduct.

The Bank shall not be liable for any direct or indirect damages that may be, in particular, caused by or in connection with:

- any error or negligence of the Client/User related to the use of E-Banking.
- the interruption, stoppage or malfunction of the E-Banking Service that might arise more particularly in case of maintenance of the computer system of the Bank,
- a virus affecting the software program made available to the Client/User and which neither the Client/User's system of protection nor the measures taken by the Bank would have made it possible to detect,
- failure to receive information as a result of a change of an e-mail address or a mobile phone number, unless it has been notified to the Bank.

11. Industrial and Intellectual Property Rights

The Client/User's access to the E-Banking Service, by virtue of the present Specific Conditions, does not create any sort of right for him/her on the overall industrial and intellectual property rights of which the Bank or a third party is the holder or licensee. Any copying, deleting, recording, imitating or falsifying, in any way, partially or in short, in any form and with any means and any defying of these in general by the Client/User, constitutes an action that is illegal, unfair and punishable by law, and which is strictly forbidden, and bringing about the sanctions of the applicable law on the Client/User.

The Client/User has the right to print, copy, or temporarily save from the Bank's website, exclusively and solely for the execution of the payment orders provided or for its own records, part or excerpts from the Bank's website and the E-Banking Service and functionalities. Any other use, such as, indicatively, the linking of the Bank's website with the website of a third party, is strictly forbidden; otherwise, the Bank is entitled to request financial compensation for any damage, whether actual or consequential, it might sustain.

The Client/User accepts that its use of the webpages on the Bank's website is consequently exclusively limited to using the Bank's E-Banking Services for their own private and personal use.

Therefore, the Client/User has an obligation to abstain from any action which has the purpose of a) reverse engineering or the reconstruction of the source code of the Bank's website software, or b) the non-authorised access of Client/User to any service, software, system, individual computer or network of computers or even record of the Bank, or c) an attack to the Bank's website and to the latter's IT system in general in any way, such as, indicatively, with the use of mechanical means or automated methods.

12. Confidentiality

The information contained, submitted or viewed on the E-Banking Service is classified and confidential by nature. The parties undertake to protect it from the access to it by any third party, and to only use it to the extent necessary.

The Client/User has duly noted that the E-Banking Service operates on the Internet, which is an international open network with characteristics and features that are well known and that entails risks that he/she accepts. In particular, although the Bank undertakes the necessary precautions as described in the "Security on Internet" section above, for the protection of the connection of the Client/User and for the protection of the

E-Banking Service, Client/User is exposed to the Internet network, therefore the Bank cannot guarantee the confidentiality of data transmitted on this network.

13. Evidence of electronic files/statements

In accordance with the provisions of and subject to the conditions laid down in the Bank' General Conditions as well as the present Specific Conditions, payment orders submitted via E-Banking are recognised as valid, binding and solid, and are considered as ones coming from the Client/User. The Client/User may not question them solely because they have not been submitted in writing or do not have an original signature.

The Client/User and the Bank expressly agree that, notwithstanding the provisions of Article 1341 of the Civil Code, the Bank is, whenever deemed useful or necessary, entitled to prove its allegations by any means legally admissible in commercial matters. The electronic records kept by the Bank have full power of proof regarding payment orders submitted via E-Banking and the applications and transactions of the Client/User with the Bank, for which the Bank is allowed to use counter proof, subject to the provisions of the next paragraph.

The transfer of money from and to an account and potential charging of fees, commissions and expenses by the Bank for payment orders submitted by the Client/User are recorded in the Bank's commercial books. Such records are kept in each individual case and are reflected in the excerpts/copies of the periodical account statements periodically sent to the Client/User carrying out any individual transaction. To specify an order, a mention indicating "by the Client/User", when he/she is submitting the order or "by the Bank", in case the Client/User does not indicate a mention himself/herself is included.

The copies of the above accounts are extracted from the Bank's commercial books and constitute full proof of the Client/User's account movement, for which the Bank is allowed to use counter proof.

14. Fees and expenses

The use of the E-Banking Service is subject to fees set out in the Bank's fee schedule, applicable as amended from time to time and advised to the Client/User through the Bank's Website or other means of communication.

15. Amendments to these Specific Conditions

15.1. Conditions of amendment

The Bank may amend the present Specific Conditions at any time by means of written notification informing the Client of regulatory changes or changes in legislation, market practices, the market situation and the Bank's policy.

The Bank reserves the right to remove, modify or add services, which are or may become part of the E-Banking Service, and to impose special and general restrictions on the use of such services.

Should the Bank intend to amend and/or add new provisions to the present Specific Conditions, the Bank will inform the Client in writing by post or on another durable medium of these amendments two months before the date of their entry into force.

In this case, a notification will be sent by the Bank via secure messaging. It is the Client's responsibility to inform the authorised Users of any such amendments.

15.2. Acceptance

Amendments of the present Specific Conditions shall be deemed to have been accepted by the Client unless

the Bank receives the Client's written opposition within two months from the date of the Bank's notification.

The non-acceptance by the Client/User of the amended Special Conditions shall be deemed by the Bank as the Client's request for termination of the provision of the E-Banking Service.

16. Duration and conditions for termination

The present Specific Conditions are concluded for an undetermined period of time. Each party has the right to terminate the provision of the E-Banking Service at any time and without having to state any reason, with one month's notice at the initiative of the Client and two months' notice at the initiative of the Bank. Such notice shall be sent by registered mail.

The termination of the E-Banking Service does not imply termination of any other contractual relationship between the Client and the Bank.

Should the Client/User fail to meet his/her contractual obligations or should the Bank have reason to believe that it may incur any liability through the continuation of its relationship with the Client or should the use of the E-Banking Service by the Client/User appear to be contrary to public order or morality, or should the Client/User fail to meet its obligation to act in good faith, the Bank may terminate with immediate effect, and without prior notice, the provision of the E-Banking Service, in which case all obligations, even obligations with a term, shall become immediately due and payable.

17. Termination of business contractual relationship

Termination of the entire contractual relationship between the Client and the Bank in accordance with the General Terms and Conditions of the Bank will automatically result in the termination of the present Specific Conditions. However, during the notice period as provided for in the General Terms and Conditions of the Bank, any Specific Conditions as well as the General Terms and Conditions will continue to apply and the E-Banking Service will remain available until the closing of the Account.

18. Miscellaneous

The present Specific Conditions constitute an Annex to the General Terms and Conditions of the Bank.

In case of any discrepancy between the present Specific Conditions and the General Terms and Conditions of the Bank, the provisions of the present Specific Conditions shall prevail.