# Online Banking - Online Access Agreement - Company / Sole Trader

| Branch | Code |
|---|---|
| | |

## Account Details

Supporting Current Account Number: ☐☐☐☐☐☐☐☐☐☐☐

Power to Bind the Company: ☐ One Signature

☐ Two or more Signatures

Transactions Authorizations Rules: ☐ Standard (They are **pre-defined rules** to facilitate the process of accession)

☐ Customized (Forces the filling of the Attachment Rules)

Note: Under Standard Rules, the movement of funds can be made with one or more signatures, depending on the power to bind the Company / Sole Trader with one or more signatures, respectively, with a limit of € 50,000 total per transaction. The necessary signatures correspond to registered Users with the ability to move funds and administer the service. When choosing Standard Rules, the profile of users is limited to the following: access to all services (viewing, handling and service administration); viewing and preparation of operations, or just viewing. If these rules and profiles do not suit your needs you can choose Custom Rules, in which case you must fill and deliver the Attachment – Transaction Authorization Rules form to the Bank, along with this Contract and the Users profile.

## Company Details / Sole Trader

Company Name / Name: _____

Tx Id Number: ☐☐☐☐☐☐☐☐☐ Share Capital: _____Euros

Adress: _____

Registered at the _____ Registry of Companies under the number_____

E-mail: _____ @ _____

## Representative(s) that bind the Company / Sole Trader

Name: _____ Tax Id Number: ☐☐☐☐☐☐☐☐☐

Name: _____ Tax Id Number: ☐☐☐☐☐☐☐☐☐

Name: _____ Tax Id Number: ☐☐☐☐☐☐☐☐☐

Name: _____ Tax Id Number: ☐☐☐☐☐☐☐☐☐

Name: _____ Tax Id Number: ☐☐☐☐☐☐☐☐☐

## User Registration Codes (To be completed by the Bank)

Identification Number: ☐☐☐☐☐☐☐☐ Registration Code: ☐☐☐☐☐☐☐☐☐☐☐☐☐☐



Mod. 10052092

**Clause 1: Scope**

1. By signing/accepting this Agreement, the Clients subscribes to the Bank's General Conditions of Use of Remote Communication Channels.
2. For the purposes of this Agreement, the following are considered remote communication channels between the Bank and the Client:
   a) Internet – the Client's access to the Bank through the web site www.millenniumbcp.pt;
   b) Mobile Channel – the Client's access to the Bank using the Mobile App service;
   c) Telephone Channel, hereinafter referred to as Contact Centre when it involves a call centre service – communication by phone established by initiative of the Client or of the Bank, including the phone contacts established through the Contact Centre (communications associated to the phone number 707504504 (domestic call) and +351210052424 (international call) or other numbers that may replace them that are disclosed by the Bank.
3. The remote communication channels are channels enabling the Client's remote access to the services that, at each moment, the Bank has available in those channels, for the celebration of legal acts and businesses within the scope of the bank relation established with the Bank, in its capacity as credit institution and insurance agent, enabling the remote access to the current account, for consultation, obtaining information and making of operations, as well as for the disclosure and trade by the Bank, and remote contracting of financial products and services, including those related with payment services, securities and insurances.
4. For the purposes of the previous paragraph, legal acts or agreements granted within the scope of the banking relationship and which may be remotely accessed by the Client are considered to be all those relating to the opening, maintenance and closing of current accounts, including the update of data from the Client and its representatives and the compliance with identification and diligence duties, payment services, credit or registration and deposit of financial instruments, as well as the procedures of signing and executing life and non-life insurance contracts and the management of incidents, including, namely, the issuance of statements regarding personal data, submission of claims or other requests, submission of requests for statements, requests of information, requests for copies of bank statements or other documents, the signing of contracts for the use of payment instruments, requests for access codes or the provision of Internet services or payment instruments, the signing of contracts for acquiring and requesting POS's, the contracting of direct debits, the contracting of money remittance services, the issuance and cancellation of payment orders, including permanent or recurrent ones, the issuance of orders on financial instruments, the subscription and redemption of investment retail products and insurance-based investment products, the request of cheques, the purchase and sale of foreign currency, the creation, reinforcement or settlement of term deposits, the subscription and resolution of rental safes, the contracting of credit operations, factoring or leasing, the issue of guarantees.
5. Through the remote channels, the Client may ask to purchase products or services with third party entities, under the terms of the agreement entered into between the latter and the Bank.
6. All agreements concluded through the Remote Channels are subordinated to these General Conditions and the to the provisions of the Documents "User's Profile" and, if the case may be, "Rules for Authorising Transactions" and to the general and specific conditions applicable to the contracting of each product or service provided, as well as to the price list in force at the Bank, applicable legislation and banking use in general.
7. The provision of services through remote channels is also ruled, in all that is not specifically foreseen herein, by the provisions of the clauses in the precedent Chapter A - Current Deposit Account General Conditions and Chapter B - Provision of Payment Services General Conditions which are deemed as herein reproduced for all purposes.

**Clause 2: Risks associated with the remote communication channels**

1. The remote channels for the access of the Client to the Bank are subject to risks of fraud by third parties, namely of "phishing", as well as to consultation and carrying out of fraudulent operations by third parties not authorized by the Client.
2. Phishing is a fraud that consists in replacing the identity of the Bank or of any trustworthy entity with the purpose of obtaining confidential information from the client, namely banking data, personal data or access codes. Phishing attacks may be made through e-mails, SMS or phone calls wherein the Bank's identity or the one from any trustworthy entity may be imitated and replaced. These e-mail messages or SMS may contain an attached file that installs malware in the Client's equipment or forwards the client to a fraudulent web page that copies or reproduces the looks of the Bank's original page, wherein the Client is asked to enter personal data and/or access codes as, for example, the User's Code, the password and/or (all) the positions of the Multichannel Code, the Authentication Code, the mobile phone number or the bank cards numbers.
3. The Client must be alert, and bear in mind that both the e-mail messages or SMS, as well as the fraudulent web page, may be quite complex and sophisticated. The Client must be suspicious of, namely:
   a) the degree of urgency of the messages threatening the client with the suspension of access to the account, of access codes or of the card if the Client's data are not supplied immediately;
   b) the request for confirmation of personal data via e-mail or SMS, namely forwarding the client for the filling in of a form for the provision of personal data and access codes;
   c) spelling/grammar errors and other errors visible in the message or in the fraudulent web page or other data that suggest the suspicious origin of the same;
   d) of e-mail messages with attached links or files;
   e) the indication that the client must supply Authorization Code(s) sent by the Bank by SMS or generated via Token, for the simulation of transactions.
4. The Client commits to read carefully and strictly comply with the safety rules and recommendations stated in ANNEX 1 - RISKS AND SAFETY RULES herein under, that is an integral part of this contract, as well as to consult and read, at least once every three months, the safety warnings and the periodical warnings disclosed by the bank at its website www.millenniumbcp.pt, including the description of the frauds attempted during that period for the fraudulent capture of the User's Code, Password/ Multichannel code and remaining customized access credentials of the Clients.
5. The Bank is in charge of ensuring that its website, Mobile Banking services and that its servers and IT components are safe.
6. The Client is responsible for the safety and reliability of the IT and communications equipment used to access remote channels, namely computers, mobile phones and internet connections owned by him/her/it or under his/her/its care, under the terms of the following numbers and the security recommendations and rules mentioned in ANNEX 1 - RISKS AND SAFETY RULES, described below.
7. The Client must possess computer and communication equipment with the appropriate characteristics to be able to access the Bank through remote channels, being his/her/its responsibility the security, maintenance and any modifications necessary to ensure permanent access to the Bank via this channel, in accordance with the technological innovations and changes that may be introduced



Mod. 10052092

and must strictly comply with the safety recommendations and rules set forth in ANNEX 1 - RISKS AND SAFETY RULES, below, as well as with the alerts disclosed by the Bank, at any moment, at the bank's website www.millenniumbcp.pt.

8. The minimum requirements in terms of equipment and communications necessary, at any time, to use each remote channel are described at www.millenniumbcp.pt, in the information spaces of each channel that the Client commits to periodically consult and to comply with diligently.

**Clause 3: Users**

1. The activation of the Client's access to remote communication channels will only be made after reception and validation by the Bank of the Document "User's Profile", and, whenever requested, of the Document " Rules for the Authorisation of Transactions", all duly filled in and signed by the representatives duly empowered to bind the Client, which are part of this Agreement for all due purposes.
2. The User (s) are natural persons appointed by the Client in the Document "User's Profile" that, in accordance with the terms and conditions therein established, may access the Bank through the remote communication means and, on behalf and in representation of the Client, carry out determined transactions, namely consultation and/or use of accounts owned by the Client, in accordance with the powers specifically defined the Client for each User.
3. As a rule, the User(s) is/are natural person(s) appointed by the Client in the Signatures Form in accordance with the usage rules and rules for the authorization of transactions therein established concerning the respective current account of the Client, except otherwise is set forth by the Client, and accepted by the Bank, in the Document "Rules for the Authorisation of Transactions".
4. Without prejudice to what is above mentioned, in the Document "User's Profile" the Client appoints the User(s) and defines, for each one, the respective profile, that is, the powers it attributes to each User, indicating, namely, the service(s) / function(s) that the User will have access to, type of digital signature and which are the accounts of the Client the User is entitled to visualise / use.
5. In the Document "Rules for the Authorisation of Transactions", the Client may also establish additional rules for the authorization of operations made by the User(s), namely the number and type of required digital signatures which are necessary to authorize the transactions, as well as define different amount brackets for the operations to be carried out.
6. The Client is totally and exclusively responsible for selecting, appointing, revoking and cancelling its Users who may be, or not, employees of the Client, as well as for the definition of the respective User's Profile, with the definition of the respective powers to act in this regard.
7. The Client hereby expressly acknowledges and accepts that the access and use by the Users, of the remote communication channels provided by the Bank, as well as the contracting of operations with the Bank by them, under the terms established hereunder, shall always be taken in all cases and for all legal effects, as being done on behalf and on account of the Client, who is always the sole Bank's counterparty in this Agreement. Likewise, and whenever the Client is a financial institution, performing banking or financial intermediation functions, it is clearly understood that the access and use by the Users, of the remote communication channels provided by the Bank, as well as the contracting of operations with the Bank by them, under the terms established under this agreement, shall always be taken in all cases and for all legal effects, as being done on behalf of the Client, which is always the sole counterparty to the Bank in this Agreement.
8. The Client is fully responsible before the Bank for the acts performed by its legal representatives and its Users while accessing and using the remote channels, in accordance with the provisions of article 800 (1) of the Civil Code.
9. For transfers and other transactions that involve the use of funds, the Client may customize transaction authorization rules through combinations of digital signature types (A, B, C or E) with a maximum of 5 combinations. All transactions implying the flow of funds shall only be executed if the requirements in terms of amounts and combination of signatures defined by the Client and previously accepted by the Bank, have been duly complied with.
10. The Client must attribute, up to a maximum of three Users, the responsibility for managing the access to the remote communication channels service, that is, it must appoint them as Administrators of the Service. It is the responsibility of the Administrators of the Service, exclusively, to: change the accounts and services / functions to which each User has access to, and the status (suspended / reactivated or removed) of each User. The Service Administrator is not allowed to make changes to his/her own profile, as well as to the other Administrators of the Service, in which case a new registry should be made by means of the filling in, signing and delivery of the Document "User's Profile".
11. The changes deriving from the previous number made by the Administrators of the Service become effective after the respective authorization by digital signature process is completed.
12. The Client may appoint new Users by identifying and registering them and sending to the Bank the Document(s) – User's Profile - duly filled in and signed by the representatives duly empowered to bind the Client. Without prejudice to what is mentioned above, the Administrator of the Service will have the power to delegate in Users empowered to make consultations and prepare operations but obeying to the rules for the authorisation of transactions that are defined by the Client for that purpose.
13. For security reasons, the Bank is authorized to eliminate users who, for more than a year, have not accessed the services and it is up to the Client to ensure that there are enough Users to keep the service running. Eliminated Users may be retrieved at the request of a Service Administrator or by the Client.
14. The Client may, at any moment, and according to his/her criteria, order the Bank to suspend/remove from certain user(s) the possibility of accessing and using the remote communication means. As soon as it receives this communication by phone, the Bank will immediately suspend the access and use of the remote communication means by the appointed User(s) and will eliminate the same only after receiving the respective written confirmation from the Client.
15. Concerning the case mentioned in the last number, the Bank will eliminate the access of the User(s) on the first banking working day following the one when the written communication therein foreseen has been received.
16. The Bank, on its own initiative, will eliminate Users in the event of duly documented statutory changes, expiration of the mandates or definitive obstruction to the exercise of their functions.

**Clause 4: Open Banking**

1. It is herein expressly agreed and accepted that, in accordance with the requirements of the Directive (EU) 2015/2366 of 25.03.2015 and the legal provisions that regulate it and transpose it, the Bank under its capacity as the provider of payment services of the Client is obliged to make the access to the above mentioned payment account(s) of the Client with the Bank available to third parties providers without the need of the establishment of any contractual relation between these and the Bank and provided that the Client gives its consent for purposes of the provision of the services of information on accounts, payment initiation and confirmation of availability of funds, better described in ANNEX 2 – OPEN BANKING below, that is an integral part of this Agreement.

2. In the document "User's Profile" the Client may, if it so desires, choose to confer powers for Open Banking service to the User(s). The management of the Open Banking service is made by the User(s) to whom the Client gave powers for that specific purpose.
3. The initiation of payments through third-party providers has, as maximum amounts per transaction, the ones defined in the Signatures Form in accordance with the rules for the authorization of transactions therein established concerning the respective current account of the Client, except otherwise is set forth by the Client, and accepted by the Bank, in the Document "Rules for the Authorisation of Transactions".
4. The Client is the sole responsible for the consent it gives to third party providers for purposes of granting them access to the Client's account(s) with the Bank, within the scope of the provision of the services of information on accounts, payment initiation and confirmation of availability of funds.

**Clause 5: Mobile App**

1. In the Document "User's Profile" the Client may, if it so wishes, choose to grant to the User(s) powers for access and use, on behalf and in representation of the Client, of the service Mobile App, from amongst the Bank's remote communication channels available, in the option "Access Level to Services".
2. In that case, the management of the service Mobile App is made by the User(s) to whom the Client has granted access to the service Mobile App, through the option "Manage Users" at the website www.millenniumbcp.pt. Namely, the User with authorized access to the Service Mobile App will be able to define/ alter a maximum amount per transaction which will function as an additional security limit in Mobile Channel, without damaging the observance of the rules set forth by the Client in the Document "Rules for the Authorization of Operations", which will prevail.
3. The Mobile App service can be used on a variety of devices. In the process of installing the service on a new device, a new User Code can be assigned specifically to that device and it maintains the same conditions initially defined for the Mobile App service. Regardless of the use of the Mobile App service on various devices, the limit set for executing transactions is non-cumulative.

**Clause 6: Codes for Client's Authentication**

1. The access and use of the Bank's remote communication channels, in accordance with the provisions set forth in these General Conditions implies the correct use of several Codes or Authentication Data in accordance with the rules established in ANNEX 1 - SAFETY RISKS AND RULES, that is an integral part of this Agreement.
2. To each User shall be attributed a User Code and a secret personal code - Password /Multichannel Access Code - which indispensable to access the Mobile and internet channels.
3. The Client may also resort to Digital Certificate(s) for access and use of the internet channel. For that purpose, the Bank makes available digital certificates, free of charge, up to a maximum of 5, valid for 1 year, that enable joining Client's Users. If the Client wants more digital certificates, it must request them to the User Support Service, but bearing the corresponding costs indicated in the Bank's pricing in effect at any time.
4. The access to the M Empresas App of the service Mobile App is made through a PIN formed by 4 numbers, which are selected in the registration process, considering the provisions of the former Clause 5 (Mobile App). In this case, as an alternative to the use of the PIN to access M Empresas App of the service Mobile App, it is possible to choose validating the access with biometric data (Face ID or Touch ID), if the device provides these technologies.
5. For the signing of specific legal acts or businesses in the remote channels, namely the making of payment operations above a determined amount by debiting the current account of the Client, an additional confirmation may be requested through a Client Strong Authentication system (AFC) or a Digital Certificate or through any other alternative mean that possesses security conditions to the ones made available by the bank for that purpose.
6. Through the services available, the Client may at any time define and manage the payment operations that, involving any type of change to their assets and/or according to the beneficiaries concerned, do not require using an AFC to be executed.
7. The Bank may at any time define a set of conditions - in relation to beneficiaries, amounts and/or operations - whose verification does not require that the Client uses an AFC to execute those operations.
8. On the website www.millenniumbcp.pt the User may alter, any time, the Password /Multichannel Code and must do so on a regular basis.

**Clause 7: Convention on proof**

1. The User Codes, the Secret Personal Codes (Password/ Multichannel Code), the Digital Certificate(s), the PIN and/or biometric data to access M Empresas App of the Mobile App service are customised security credentials that allow the Bank to verify the identity of the Client, authenticate the respective access and use of the remote channel and establish the validity of the orders therein transmitted, being an e-signature, object of an individual and exclusive right of the Client, the use of which in accordance with what has been agreed, identifies and authenticates the Client before the Bank and constitutes evidence that the instructions and e-documents transmitted this way to the Bank were made by the Client.
2. The parties accept the legal equivalence of the security credentials mentioned above, as well of the Mobile Digital Key to the Client's handwritten signatures.
3. All requests for information, transmission of orders, instructions, or contract signing or signing of any legal acts or businesses using the above mentioned customized security credentials under the terms agreed hereunder, will be construed by the Bank as being made by the Client and the Bank will not be required to verify the Client's ID in any other way.
4. The provisions set forth in the previous number cannot be interpreted as able of preventing the Bank from obtaining confirmation from the Client concerning the orders or instructions received, including a written confirmation, with a handwritten signature, nor damage the adoption of another way to formalize the banking transactions at the Bank's request or due to a legal requirement, or limit the acceptance of a specific type of instructions in view of amounts, number of orders or other criteria.
5. The orders and instructions that the Bank receives, as well as the acts of underwriting of contracts provided that they are properly validated through the use of the customized security credentials mentioned above enjoy full legal effect, the Bank remaining irrevocably entitled to fulfil and execute them and to carry out the debits and credits arising from them, it being understood, in any case, that the Bank acts to comply with the orders and instructions given by the Client and with its real wishes.
6. It is hereby expressly agreed between the Client and the Bank that, under the terms and for the purposes of article 3 (4) of Decree Law 290-D/99, of 2 August, the correct use of the above mentioned customized security credentials of the Client shall have the same legal value as and serve as proof of the Client's legal representatives handwritten signature on paper.
7. The provisos of the foregoing and of this clause also apply to the contracting of products or services with third party entities, as set out in clause 1 (5), the Bank acting, under this provision, on behalf of and in representation of those entities.

**Clause 8: Duties and responsibilities of the Client**

1. The Client commits to take all reasonable care and diligence measures necessary to preserve the security and secrecy of the security customized credentials indicated in 1 of the precedent clause 7 for purposes of authentication before the bank, not allowing nor facilitating the same to be known by third parties and commits to keep them confidential and make a careful, attentive and strictly personal use of the same.
2. The Client is responsible for the correct safekeeping, use and maintenance of the customized security credentials mentioned in 1 of the previous clause 7, for purposes of authentication before the Bank.
3. Namely, the Client commits to adopt all precautions and reasonable and appropriate measures so that the Code(s), the Secret Personal Codes (Password/Multichannel Access Code) the Digital Certificate(s), the PIN and /or biometric data to access to the M Empresas App of the Service Mobile App do not become accessible or able of being perceived by third parties. The Client should not write them down in a way that is easily accessible to others, not even in the mobile phone, mobile equipment or computer nor in any other document or support that the Client keeps next to them.
4. The Client must remain attentive, be cautious and consider the risk of receiving e-mail messages, SMS or even phone calls with fraudulent purposes wherein the Bank's identity is imitated and replaced to, in a deceitful and fraudulent manner get from the Client its customized security access credentials. Namely, the Client must suspect the level of urgency of the messages requiring an immediate action or threaten, for example, with the suspension of the access if the access credentials are not immediately supplied or the request for the confirmation of data, namely instructing the client for the online filling in of personal information forms and supply of access codes and credentials or SMS and e-mail messages with links or attached files to download and install.
5. The Client commits to read carefully and strictly comply with the safety rules and recommendations stated in ANNEX 1 - RISKS AND SAFETY RULES that is an integral part of this Contract, as well as to consult and read, at least once every three months, the safety warnings and the periodical warnings disclosed by the bank at its website www.millenniumbcp.pt, including the description of the frauds attempted during that period for the fraudulent capture of the customized access credentials of the Clients.
6. The Client commits to access and use the remote communication channels of the Bank in accordance with the clauses and terms and conditions that rule the respective use and to communicate to the Bank, without any unjustified delay, as soon as the following happens:
   a) If at any time the Client becomes aware or has reason to suspect the loss and/or improper access or use by a third party(s) of the personalised security credentials of one (or more) User(s), namely of User's Code(s), Password(s), Multichannel Access Code, Digital Certificate(s), PIN and/or biometric data to access the M Empresas App of the service Millennium Mobile App, and/or;
   b) If at any time the Client has reason to suspect of the use by a third party(s) of the customised security credentials of one (or more) User(s), namely User's Code(s), Password(s), Multichannel Access Code, Digital Certificate(s), PIN and/or biometric data to access the M Empresas App of the service Millennium Mobile App, and/or;
   c) Suspects of undue access by third parties to its email address and/or computer, mobile phone or portable device or mobile phone number by any way whatsoever and/or;
   d) Becomes aware of the of loss, misplacement, theft, or misappropriation of the mobile phone where the M Empresas App is installed; and/or
   e) Verifies the recording in the deposit account of the Client of any non-authorized transaction or the existence of errors and irregularities in the making of transactions.

   In any of these cases, the Client shall immediately contact the Bank, by telephone to 21 427 04 02, a permanent call centre open 24/7, 365 days/year, to warn Millennium bcp and request the blocking/prevention of abuse or fraud against it. Moreover, the Client should confirm the facts reported to the bank in writing and within 5 calendar days.
7. The Client is fully responsible before the Bank for the acts performed by its legal representatives and its Users while accessing and using the remote channels, in accordance with the provisions of article 800 of the Civil Code.
8. Accordingly, it is clearly understood that it pertains exclusively to to Client to select very thoroughly its Users and instruct and provide each one with the knowledge and means necessary to access and use the remote Communication Channels of the Bank, in accordance with the provisions established hereunder, with the Document(s) "User's Profile" and, if the case may be "the Document Rules for the Authorization of Operations", as well as convey to them the security recommendations and rules set forth in ANNEX 1 - RISKS AND SAFETY RULES, hereto attached and an integral part of this Agreement. Namely, the Client commits to:
   a) Give to each User specific instructions and information on fraud risks, namely "phishing", alerting the User for the need to be careful, attentive and cautious, providing to all Users information and the alert signs detailed in number 4 above; and
   b) Provide each User with a copy of ANNEX 1 - RISKS AND SAFETY RULES, hereto attached and an integral part of this Agreement, ensuring that the User reads the same attentively; and
   c) Ensure that each User consults and carefully reads, at least once every three months, the safety warnings and the periodical warnings disclosed by the bank at its website www.millenniumbcp.pt, including the description of the most common frauds attempted during that period for the fraudulent capture of the customized access credentials and that it remains duly informed and updated on the precautions and care rules to adopt; for such the Client should instruct each User in that sense and ensure the periodical compliance with those instructions; and
   d) Instruct and alert each User for the fact that the respective User's Code, Secret Personal Code (Password /Multichannel Access Code), Digital Certificate, PIN and/or the biometric data to access the M Empresas App of the service Mobile App are personal and not transferable, informing it of all the all reasonable care and diligence measures which must be adopted to preserve the possession, security and exclusive, reserved and confidential use of the same, in representation and on behalf of the Client; and
   e) Instruct and alert the Users to whom it granted powers to use the Service Mobile App that they must adopt all reasonable care and diligence measures to preserve the possession, the security, and the exclusive, reserved and confidential use, at each moment, of the mobile phone or mobile equipment wherein the M Empresas App is installed; and
   f) Inform each User that it may, at any time and using the website www.millenniumbcp.pt, alter the Password / Multichannel Acces Code attributed and inform the User that it may do so periodically; and
   g) Instruct each User in the sense that it must access and use the Bank's remote communication channels in accordance with the clauses and rules that rule the respective use; and
   h) Instruct and alert each User that it must communicate to the Client and to the Bank, without unjustified delay, as soon as the it becomes aware or suspects of the occurrence of some of the facts indicated above in number six of this Clause, namely the loss, theft or misappropriation, or any unauthorised use of the customized security credentials, namely of the User Code(s), Personal Secret Code (Password / Multichannel Access Code), the Digital Certificate, PIN and/or other biometric date to access

the M Empresas App of the service Mobile App Millennium, and/or of the Client's e-mail address, and or mobile phone or mobile equipment wherein the M Empresas App is installed, or the mobile phone number associated, by any means, and must immediately contact the Bank by calling 21 427 04 02, a permanent call centre open 24/7, 365 days/year, so as to warn Millennium bcp and request the blocking/prevention of abuse or fraud against it; and

i) Ensure that the Users commit to observe the instructions and duties mentioned in the precedent paragraphs of this number.

9. After the communication from the Client, made in accordance with the provisions of number six of this clause, the Bank shall block the access to the Client's accounts through the remote communication channels.
10. The provisions of clause 12 (Unauthorised or incorrectly executed operations) and 13 (Liability for unauthorised operations) of the previous Chapter B - Provision of Payment Services General Conditions apply here and are deemed as herein reproduced for all purposes.

**Clause 9: Handling of the Client's Instructions**

1. Without damaging the provisions of Clause 11 (Suspension, blocked access and termination of the Agreement) below, the Client may give instructions to the Bank through the remote communication means at any time of the day, every day of the year.
2. The execution of the orders given by the Client will be carried out in accordance with the conditions applicable to the type of remote channel in question, service or product requested.
3. The Bank may refrain from executing orders transmitted by the Client where they do not respect applicable statutory provisos or conflict with banking practices, when the account concerned does not have sufficient funds for the intended operation, or when any provision shown in these General Conditions and in ANNEXES 1 and 2 as well as in the Document(s) "User's Profile", the Document "Rules for the Authorization of Operations" and, if the case may be, other documents applicable to the service are not fulfilled, or due to some irregularity in the process of transmitting and/or authorising the order in question that is not properly remedied within 72 hours.
4. Once authorised and sent to the Bank for immediate processing, no alterations may be made, nor may the transmitted orders be cancelled via the remote communication channels.
5. The orders transmitted on non-working days shall be considered as having been given on the immediately following working day. The client must always comply with the time limits set by the Bank for processing orders on the same day for the various products and services.
6. The "BancoMail" function of the internet channel does not obligate the Bank to execute the orders, unless this is expressly agreed.
7. Considering that the services and/or operations provided by the Bank through the remote channels shall be subject to interferences, interruptions, disconnections or other anomalies, namely in the event of breakdowns, power surges or other events outside the Bank's control, the Client expressly accepts that the Bank shall not be liable for current or potential damage or losses, including future earnings, that may directly or indirectly result to the Client from such events, in the extent that those interferences, interruptions, disconnections or other anomalies have been originated by acts or omissions from third parties, as well as bank's suppliers or services license providers and in services held and controlled by them.

**Clause 10: (Recording of operations and provision of statements, Transaction Slips and Invoices)**

1. The Client and the Bank agree that the computer recording of operations carried out under this Agreement, which may be viewed on screen and/or printed on paper, constitutes appropriate evidence of the orders given by the Client.
2. The Bank undertakes to maintain the information it provides to the Client via the Internet and Mobile channels permanently updated. However, the Bank's own accounting records shall always take precedence over this.
3. The Client expressly accepts that the combined statements and of entries, the transaction slips and invoices to be provided electronically and such e-documents may be viewed on screen and/or printed on paper.

**Clause 11: Suspension, blocked access and termination of the Agreement**

1. The Bank may inhibit and block, totally or partially, the access and use of the remote communication channels by the Client due to objectively grounded reasons related with:
   a) Threat to safety, or for reasons due to assistance, maintenance, repair or introduction of improvements to the security of the remote communication channels;
   b) The suspicion of unauthorized or fraudulent use of that instrument by third parties;
   c) Significant increase of the risk that the Client might not be able to comply with its payment liabilities, if involving an associated credit line.
2. In accordance with the circumstances of the case, the following reasons may constitute situations able of being framed within one of the paragraphs of the previous number:
   a) When there are founded security reasons and, namely, if the Bank is informed or is aware that one or more of the customized security credentials have been lost, misplaced, robbed, stolen or abusively appropriated;
   b) If the Bank is aware or suspects of any fraudulent use or of any irregularity which might result in a serious harm to the Payments System, to the Bank or to the Client;
   c) If the Client is inhibited from using cheques, or if, for any other grounded motive there is a significant increase in the risk of the Client not being able to meet credit liabilities;
   d) If the balance of any Current Account of the Client is unavailable due to foreclosure, seizure, inventoried, pledged, freezing, bankruptcy, insolvency or any other apprehension by court and/ or judiciary or supervisory authorities order.
3. In the cases mentioned in number 1 above of this clause, the Bank should inform the Client of the blockage and respective justification by e-mail or any other expedite mean, if possible before blocking and, at the latest, immediately after the blocking, except if such information cannot be provided for security reasons objectively grounded or it is forbidden due to other applicable legal requirements.
4. As soon as the motives that led to the blockage cease to to exist, the Bank will remove the blockage.
5. For security reasons, the User will be prevented from accessing Bank services through the Internet and Mobile, after three consecutive failed attempts to enter the respective User Code, Password /Multichannel Access Code. In this case, the re-activation of the access may be obtained through a written communication duly signed by the Client requesting the re-activation of the User, a direct request made by the User at any Branch of the bank or any other equally safe method communicated by the Bank for that specific purpose.
6. This agreement for accessing and use the remote communications channels may be terminated by any of the parties, as generally permitted by law. Without damaging the provisions of the precedent clauses, the Bank may terminate this Agreement - General

Conditions of Use of Remote Communications Channels and immediate cancel the access and use of the remote communication channels by means of a written communication and this communication will be presumed as received by the Client on the third calendar day after its postal remittance, in any of the following cases:

a) Due to any of the motives and facts mentioned in the paragraphs of the precedent number two;
b) The customer, in any way, interrupts its corporate activity, considerably reduces its solvency guarantees or presents a project for voluntary winding up;
c) The Client submits to insolvency or is required to submit its insolvency;
d) The Client applies for a Special Revitalization Process;
e) The authorization for the Client to undertake its activities is revoked;
f) If any corrective, provisional administration or resolution measure is applied to the Client;
g) When it is verified that information provided related with claim(s) presented to the Bank on the access and/or use of the remote communications channels are false or incorrect;
h) If any precautionary measure is requested concerning the suspension of corporate resolutions of the Client and/or destitution of managers or of a member of the Client's management body;
i) If the existence of any litigation or lack of understanding and of consensus amongst the members of the management body of the Client is reported to the Bank by any of them or if the Bank receives contradictory instructions given by any of them under circumstances that show lack of cohesion or understanding amongst the members of the management body of the Client.

**Clause 12: Financial information**

1. The financial information available through the Internet and Mobile channels, namely prices, indexes, news, studies or other, is provided by the Bank solely for information purposes and is drawn up by third parties which authorize the Bank to disclose it to Customers.
2. Despite the careful selection made by the Bank concerning its sources of information, errors or omissions may not be detected by it; hence, the Bank cannot guaranty the accuracy of the disclosed information nor be deemed liable for the incorrect use or interpretation of such information.
3. The Client shall use the disclosed financial information at his/ her own account and risk and will be exclusively responsible for the investment decisions made based on such information.

**Clause 13 Service costs**

1. The Client authorizes the Bank to debit the current account identified hereunder near the signatures and date of this Agreement, for the costs relating to services and transactions made through the remote communication channels, including those concerning the purchase of goods or services from other suppliers on the internet channel and Mobile, and hereby authorises the Bank to, in the event of insufficient balance and if it so wishes, but without being obliged to do so, debit the above mentioned account in the necessary amounts or to debit any other account that the Client holds or will hold with the Bank.
2. The operations that the Client carries out with the Bank through internet and mobile channels and also the utilisation fees due are subject to the provisions of the Bank pricing in effect at any moment. The Bank may, at any time, change its pricing. The Client shall be informed of the changes introduced in the pricing by circular letter, message on the account statement, electronic mail or other appropriate means agreed by the parties. The amendments proposed by the Bank shall come into force after at least 30 days written notice is given to Client, and, should the Client not agree with the proposed amendments, they may state in writing their intention to terminate the contractual relationship within a maximum of 30 days of being informed by the Bank of the amendments, being assumed that it accepts the same them if it does not do that.
3. The Client shall bear no costs for contacts initiated by the Bank without prejudice to the price or charges due for the financial service engaged pursuant to each contact.

**Clause 14: Early termination, alteration of the Agreement and Resolution**

1. The Bank can propose changes to the clauses of this Agreement, arising from legal requirements or related to international systems and security rules or when deemed suitable by the Bank.
2. This (these) change(s) will be communicated to the Client on a durable media sent to the e-mail address of the Client or through prior notice or a message inserted in the statement of the Card Account and/or Associated Current Account, by circular or other appropriate means normally used, at least two months in advance of the date of its application.
3. It is expressly agreed that, in the subsequent silence of the Client, it is deemed that it tacitly accepts the change(s) thus proposed by the Bank, unless, prior to the entry into force of such proposal, the Client notifies the Bank that it does not accept them.
4. If the Client does not agree with the proposed change(s), the Client may immediately terminate this Agreement - General Conditions of Use of Remote Communications Channels provided that the Client informs the bank immediately before the entering into force of the proposed changes(s) and in writing.
5. This Agreement - General Conditions of Use of Remote Communications Channels may be early terminated any time, effective immediately, by the Client through a communication in writing addressed to the Bank.
6. This Contract may be early terminated by the Bank by means of a two-months prior notice from the date on which the early termination becomes effective.

**ANNEX 1 - RISKS AND SAFETY RULES**

**General rules for accessing/using of all the remote communication channels of the Bank**

1. The Client commits to read carefully and strictly comply with the security rules and recommendations stated herein, as well as to consult and read, at least once every three months, the security warnings and the periodical warnings disclosed by the bank at its website www.millenniumbcp.pt, including the description of the frauds attempted at any time for the fraudulent capture of the User's Code, the Multichannel code and remaining customized access credentials of the Clients.
2. The Client must beware and be prepared against fraud attempts by unauthorized third parties. In particular, the Client should beware of any e-mail that requires "immediate action" or creates a sense of urgency, especially if it shows spelling errors or bad grammar and has attached links and/or executable files.
3. Millennium bcp never sends e-mails or SMS with links and never requests the confirmation of the Client's personal data or confidential nor codes or authentication data to access bank accounts vis these communication means, namely instructing the client for the online filling in of personal information forms and supply of access codes and credentials. If such happens, the Client must consider that it may well be a fraud attempt.

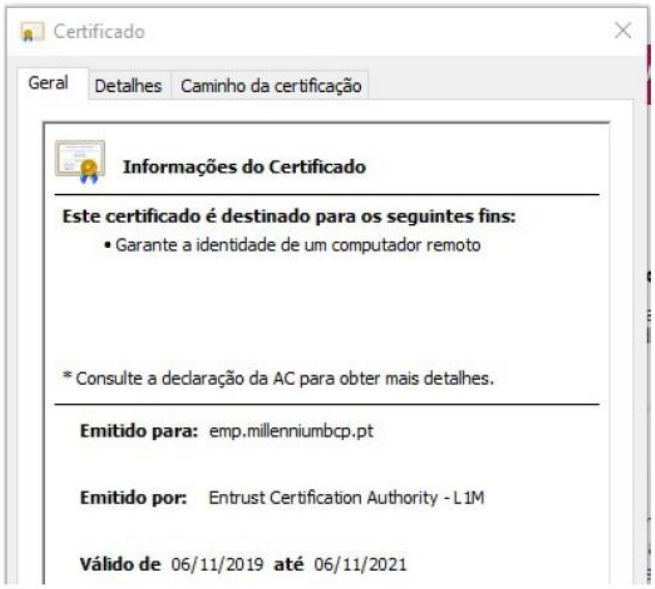
4. The Client should analyse the e-mails received before opening them, always confirming the source and the subject, if possible, with the issuer entity. The Client should not accept the execution of programs the download of which is activated without his/her request.
5. If at any moment the Client receives an Authentication Code to confirm a transaction that the Client did not request, the Client should refrain from entering or disclosing that code and must immediately report that fact by calling 707502424 / 918272424 / 935222424 / 965992424 (domestic call) or +351707502424 / +351210052424 (international call) a permanent client assistance centre – 24/7, 365 days/year, so as to warn the Bank and request the locking/prevention of abuse or fraud against it.
6. The Client must never disclose the Authentication Code(s) to third parties under any pretext and commits to make a cautious, prudent and exclusively personal use of the same, assuming all risks and consequences deriving from their undue disclosure.
7. If, at any moment, the Client verifies that its mobile phone is inactive and that the mobile phone number is not functioning properly, the Client must immediately contact its telecommunications operator and ensure the correct functioning of the SIM card linked to its mobile phone number supplied to the Bank.
8. If, at any moment, the Client:
   a) Becomes aware or has reason to suspect the loss and/or improper access or use by a third party(s) of the personalised security credentials of one (or more) User(s), namely of User's Code(s), Password(s), Multichannel Access Code, Digital Certificate(s), PIN and/or biometric data to access the M Empresas App of the service Millennium Mobile App, and/or
   b) If at any time the Client becomes aware or has reason to suspect the loss and/or improper access or use by a third party(s) of the customised security credentials of one (or more) User(s), namely User's Code(s), Password(s), Multichannel Access Code, Digital Certificate(s), PIN and/or biometric data to access the M Empresas App of the service Millennium Mobile App, and/or
   c) Suspects of undue access by third parties to its e-mail address and/or mobile phone, computer, or portable device or mobile phone number by any way whatsoever,
   d) Becomes aware of the loss, misplacement, theft, or misappropriation of the mobile phone where the M Empresas App is installed, and/or
   e) Verifies the recording in the account of any non-authorized transaction or the existence of errors and irregularities in the making of transactions.

   Then, the Client should, immediately, contact the Bank by calling 707502424 / 918272424 / 935222424 / 965992424 (domestic call) or +351707502424 / +351210052424 (international call), a permanent client assistance centre – 24/7, 365 days/ year, so as to warn the Bank and request the locking/prevention of abuse or fraud against it. The Client should also confirm what happened before the Bank, in writing and within 5 days.

**Additional rules to access the website www.millenniumbcp.pt:**

1. Whenever you access your bank accounts using Millennium bcp Website, make sure that: (i) if the address starts with https:// emp.millenniumbcp.pt/, (ii) if the address bar is green and (iii) if, at the end of the address bar, a lock is shown followed by "Millennium BCP" as shown:


2. In case of doubt, confirm the origin of the digital certificate - double click on the padlock - and check if it effectively identifies Millennium bcp:




3. The access to the website www.millenniumbcp.pt may be made by 2 ways:
   a) Identification of the User Code, password and two (2) random digits of the tax identification document (which will always be the same until login is successful);
   b) Identification of the User Code and three (3) random positions of the Multichannel Access Code, which will always be the same until login is successful.

   Therefore, if additional information is requested it is an attempt to commit fraud and you should report it immediately by calling 707 50 24 24. From abroad call +351 210 04 24 24. Personal assistance available every business day from 8 a.m. to 2 a.m. (GMT) and on non-business days from 10 a.m. to 24:00 (GMT).
4. While the Client accesses the website www.millenniumbcp.pt the Bank never requests the mobile phone number or the installation of software/security programs.
5. Millennium bcp always sends SMS and e-mails with no links.

6. The Client should never open Millennium bcp's website through links on messages, search engines or even through the option "Favourites". Always type in the complete address www.millenniumbcp.pt to avoid accessing untrustworthy pages, very similar to Millennium bcp's website, as well as to avoid the installation of malware in the equipment used to access Millennium bcp's website.
7. Millennium bcp never requests personal and/or confidential data, as for example the Password/Multichannel Access Code, mobile phone number, change of data, etc. by email, SMS or by any other mean.
8. Don't trust e-mails, allegedly sent by Millennium bcp requesting personal and/or confidential data, as the Multichannel Code, the Confirmation Key, the telephone number, etc. Millennium bcpnever requests this type of information to its Clients, by e-mail, by SMS or by any other mean.
9. The Client should carefully read the SMS received containing the Authentication Codes since the transaction data are identified in the text message. Never give to third parties the Authentication Codes received via SMS or via token.
10. Don't use obvious Password/Multichannel Access Codes (1234567; 1111111; date of birth; etc) to access the website www.millenniumbcp.pt. Alter the codes to access Millennium bcp periodically, in "Other Services» Management of Personal Data: Alter Password/Multichannel Access Code"
11. Define unique Access Codes for the website www.millenniumbcp.pt and don't use them on other websites.
12. Never give third parties personal identification data that can be used for certification with the mobile phone operators, or User Codes, Multichannel Access Codes or other codes, namely authorisation codes received by SMS or Token.
13. The Client should also prevent third parties from accessing the equipment used to confirm banking operations as well as their components, such as SIM cards.
14. Should the Client suspect that its access codes have been compromised, it should change them as soon as possible or request that they be blocked using the Bank's phone channel.
15. Millennium bcp will never, under no circumstance, request simultaneously more than 3 digits of the Multichannel Code.
16. The Client should keep its computer(s) protected and should commit, to, namely:
    - Install a good anti-virus and keep it constantly updated:
    - Use a firewall to filter Internet traffic in and out of the computer;
    - Pay attention to the security updates that credible software companies provide and install them according to the instructions given;
    - Always use updated versions of browsers and operating systems;
    - Deactivate the options save the password and browser autofill;
    - If the computer is shared with someone else, the Client should beware and always apply basic protection measures: close the browser window or always end each session and delete the cache memory;
    - The Client should not open e-mails with an unknown origin and especially should not click on or open attachments or links appearing in those messages;
    - The Client should not open files sent by unknown senders;
    - The Client should keep himself/herself up-to-date on general safety concerning the use of internet.
17. Always read the Bank's newsletters and the information we provide you on security at www.millenniumbcp.pt. Please feel free to suggest any security issue you would like to read about on our newsletter. Whenever the Client has any doubts or if it needs further information, please e-mail us to empresas@millenniumbcp.pt or call us on 50 45 04. From abroad call +351 210 04 24 24. Personal assistance available every business day from 8 a.m. to 2 a.m. (GMT) and on non-business days from 10 a.m. to 24:00 (GMT).

**Additional Rules to access the Contact Centre service**

1. The Bank's phone service for:
    a) Support for Company's users is available by calling 707 50 45 04. From abroad, call +351 210 04 24 24. The service is personalized and the User Code and/or the Tax Identification Number (TIN) of the Company / ENI are requested;
    b) Support for Company's users is available by calling 707 50 24 24. From abroad, call +351 210 05 24 24. The service is personalized, and you will be asked to enter your current account number and 3 random positions of the Multichannel Access Code.
2. To carry out some transactions or to change personal data, additional security data (personal or related to the Bank) may be requested.

**Additional rules of access to Mobile Service App**

1. The Client should:
    a) Activate a form of automatically blocking its mobile equipment and of unblocking it by means of a secret code or biometric data of the User;
    b) Protect its smartphone/tablet with a good antivirus, keeping the same always updated and operational;
    c) Pay attention to the security updates that credible software companies provide and install them according to the instructions given;
    d) Deactivate the option for the installation of apps with unknown origin in the security settings of your equipment;
    e) Always resort to the official websites /stores when needing to install any app and be cautious before making the download of an app, read the opinion from other users and verify which tools and permissions the Client will have to give access to in his/her equipment (ex: reading and sending of sms, access to contacts, location). It is crucial that the Client pays attention to the permissions it grants to the apps it installs in its mobile equipment;
    f) When using the e-mail in its mobile device the Client must certify that it never accesses messages that the Client does not recognise, mostly attachments or links appearing in those messages. In case the Client receives any suspicious e-mail allegedly sent by the Bank, the Client should not open the same and report the fact to the Bank by calling 707502424 / 918272424 / 935222424 / 965992424 (domestic call) or +351707502424 / +351210052424 (international call),a permanent client assistance centre – 24/7, 365 days/year, so as to warn the Bank;
    g) The Client must bear in mind that Millennium bcp never sends e-mails and SMS with links;
    h) The Client must bear in mind that free Wi-Fi networks facilitate access by third parties to his/her mobile phone and to its data and communications. The Client should not use public Wi-Fi networks to access the website or mobile channel of the Bank nor to access websites requiring the entering of sensitive information, make online purchases and homebanking. For this type of accesses, use always and only the data network of the mobile equipment;
    i) Deactivate the Bluetooth when it does not need it since the mobile phone will be less vulnerable to cyber-attacks;
    j) Keep the smartphone/tablet physically safe and under constant surveillance.

2. The apps of Millennium bcp to be installed and used in mobile phones are available for Apple and Android TM devices. Install the apps through the brand's official web stores (Apple Store and Play Store). Never do so using links provided to you by third parties, namely by e-mail or by SMS.
3. M Empresas App Registration:
   After installing the M Empresas App, define the Security PIN, composed of 4 numbers and do not use it in other Apps. Afterwards, enter the User Code and request the sending of the SMS Code, indispensable for the registration of the App; enter, as usual, the three (3) random positions of the Multichannel Access Code or your password to validate the remittance of the SMS. Finally, enter the code you received by SMS and validate with more three random positions of the Multichannel Code or your password.
   Millennium bcp will never, under no circumstance, request simultaneously more than 3 digits of your Multichannel Code.
4. Access to the M Empresas App:
   4.1 The login to the M Empresas App is made using a 4 digit PIN code defined during the registry.
   4.2 As as alternative to the use of a PIN, you can login to the Millennium APP using fingerprint or facial recognition (FaceID or Touch ID), if the device provides these technologies. In the login page you will always have the possibility of accessing using the fingerprint, facial recognition or through the PIN. To activate/deactivate access to the M Empresas App through Touch ID or Face ID just go to "Settings".
   4.3 When turning on the Touch/Face ID on the M Empresas App, the User should:
   a) Ensure that the biometric data (Fingerprint/Face Recognition), recorded on personal mobile device are yours alone;
   b) Inform the Bank whenever it finds that its Touch/Face ID authentication device was compromised, authorizing the Bank to immediately block access to the channel until the situation is solved;
   c) Beware that the mobile device's existing fingerprint/face recognition authentication module is not property or provided by the Bank, therefore the Bank cannot guarantee that access using this means of authentication is secure, nor can it be held liable for an eventual malfunction or inherent losses arising from the use of this form of authentication.
5. For the making and confirmation of transactions, M Empresas App will never ask, simultaneously, more than 3 digits of the Multichannel Access Code or Password to confirm transactions. Therefore, if additional information is requested it is an attempt to commit fraud and you should report it by calling 707 50 45 04. From abroad call +351 210 04 24 24.

**Risks**

Failure to comply with the recommendations on the use of distance communication means issued above may lead to the following risks for the users:
- Third parties may gain access to personal and confidential data;
- Third parties may execute transactions using the assets in the account and generate financial losses.

**ANNEX 2 – OPEN BANKING**

1. It is up to the client to assess if he/she wishes to share or not his/her banking data. Open Banking affords the client the possibility to share with third parties balances and transactions of accounts held at the Bank but only if the Client gives his/her express consent.
2. If the client considers suitable that certain institutions or payment service providers, without any contractual connection with the Bank (third parties payment services providers - TPPs) have electronic access to the payment account balance held at the Bank, as well as to other financial information of the account, or start using the account to make payments, the client may contract with these institutions or operators some of the following Open Banking services:
   - Payment Initiation Services;
   - Account Information Services;
   - Balance Confirmation Services.

   The payment Initiation Services allow for a TPP to set up a payment order in the account which the client holds at the Bank (ex. an online payment directly in the client's account to the TPP account).
   The information Services on the accounts allow a TPP to gather in its website, financial information from several accounts, including balances and transactions of the account the Client holds at the Bank (financial institutions or entities that run price comparison sites will be among the companies that provide this type of service).
   Balance confirmation services allow a TPP issuing card-based payment instruments, at the time the Client makes a card payment, to confirm that the account held with the Bank has enough balance to make the payment.
   The possibility for a TPP to provide the services mentioned above, requires that the account held at the Bank is accessible in the digital channels of the Bank and consequently, the prior subscription by the Client to the current Agreement for the Use of Remote Communications Channels.
   The Bank is obliged to make the IBAN of the account held by the client at the bank available to the TPP and, depending on the case, the respective balance or the balance and transactions, or to accept the payment operation initiated by that party, and the TPP does not have to identify the Client nor to make proof of the contract signed with him/her to provide Open Banking services and have direct access the Bank.
3. It is the Client's responsibility, once redirected to the Millennium bcp website/app, to confirm the authorisation given to a TPP to provide certain Open Banking services and have direct access to the Bank, and he/she should to that effect, at www.millenniumbcp.pt, correctly introduce the User Code, three random positions of the Multichannel Access Code and an Authentication Code sent by SMS to the phone number registered at the Bank or obtained viaToken or, in the M Empresas App, to correctly introduce the Security PIN made up of four numbers and an Authentication Code sent by SMS to the phone number registered at the Bank. Therefore, if additional information is requested, it is an attempt to commit fraud and the same should be reported by calling 707 50 24 24. From abroad call +351 210 05 24 24.
4. The User Code, the Password/Multichannel Access Code and the PIN, indicated in ANNEX 1 - RISKS AND SAFETY RULES of these General Conditions, are personal, confidential and not transferable authentication data and therefore the client cannot allow their use by third parties, using them in a strict and exclusively personal manner.
5. Before deciding to share with third parties the balances and transaction of the accounts held with the Bank, the Client must take the necessary steps to confirm that the TPP is a legitimate entity, namely whether it is a registered entity with Banco de Portugal or the National Competent Authority of the country of origin.
6. It is the TPP's obligation to provide clear and objective information about its identity and contact details, purpose and basis for the processing of information concerning the Client, the recipients of the data if there are any, the fact that it intends to transfer data to a third country, if that is the case.

7. The Client must take into consideration that if he/she decides to give consent to TPPs to access bank data and if, in addition, confirms in the Millennium bcp website/app the authorisation given to a TPP to provide a certain Open Banking service and have direct access to the Bank, the Bank cannot guarantee the way or the purpose in which that information will be used by it, and because it is a payment Initiation Service, the transaction is therefore authorised, and the consent given for its execution cannot be cancelled. Notwithstanding, after the client's consent, under the terms mentioned above, and having had access to bank data that concerns it, the TPP is solely responsible for the security of the data thus obtained.
8. The client should bear in mind that he/she can manage and cancel the authorisations for Open Banking provision of services given to the TPPs at the website/Millennium bcp app, by accessing the Area M toolbar at www.millenniumbcp.pt. The Client can also call the Millennium bcp Helpline.
9. In any event, under the law, the Bank has the prerogative to refuse access by a TPP to the Client's bank details if it considers that there is a risk of fraud.

## Signatures and Stamps

Date _____ / _____ / _____
Year Mouth Day

Customer

_____

_____

_____

_____

**Signatures Verification**
The signature of the Representative or Representatives that bind the Company match our files.

Date_____/_____/_____

Sign:_____

**Banco Comercial Português, S. A.**
(Bank's Authorized Signatures)

_____ _____

NUC _____ NUC _____



Mod. 10052092