General Conditions

The contract is concluded between:

Our website address is: https://tic.business

Payment service provider

TiC Global Payments, S.L. the service provider is a Spanish company with a registered office at Avenida General López Domínguez Ed. Puerto Azul portal 2A Entreplanta oficina 1, 29602 Marbella (Málaga) Spain with NIF: B93746741 registered in the company registry of Málaga.

The collaborating company that provides the Payment Services is PECUNIA CARDS EDE, S.L.U. (the "Electronic Money Entity"), a Spanish company with registered office at Calle Guzmán El Bueno, number 133, Edificio América, Bajo B, 28003 Madrid, provided with NIF: B-86972346, and is registered in the "Registro Mercantil de Madrid". The Electronic Money Entity is subject to the supervision of the Bank of Spain and is registered in the "Registro de Entidades de Dinero Electrónico del Banco de España" under the number 6707.

General conditions of payment services

Hereinafter referred to as "**the Institutions**" on the one hand,

And

The Customer, (i) a legal person or (ii) a natural person acting on their own behalf for professional purposes, registered or resident in a Member State of the European Union, specifically the SEPA countries.

Hereinafter referred to as "**the Customer**", on the other hand.

Together referred to as the "**Parties**".

Warning

The prospect is invited to carefully read this Contract sent online by the Institution before accepting it.

The subscription to the TiC Business offer is made entirely online by the customer on the Site or the Application.

The Customer accepts the Contract without reservation by signing it electronically.

The Customer may at any time consult it, reproduce it, store it on their computer, or on another medium, send it by email or print it on paper so as to keep it.

By checking the box "I expressly consent to the processing of my personal data, "the Customer further explicitly agrees that the Institutions will access personal data necessary for the performance of the Services, process them and retains them in the manner specified in the article "Personal Data".

The Contract and its appendices are written in English and Spanish. In case of divergence of interpretation, only the English version shall prevail.

Terms of services

1.Definitions

The terms of this Contract used with the first letter capitalised shall have the meanings defined below, regardless of whether they are in singular or the plural.

Website or Application

Refers to the Website or Application provided by the Institution to give access to the Personal Area.

Simple authentication

Refers to the procedures defined by the Institution to verify the identity of a User or the validity of a Payment Order. These procedures include the use of personalised Security Data and Credentials.

Strong authentication

Refers to the procedures defined by the Institution to verify the identity of a User in accordance with the provisions of the Monetary and Financial Code. Strong Authentication includes elements to establish a dynamic link between the Operation, the amount and the Beneficiary.

Administrator

Designates a natural person, mandated by the Customer, having all the rights on the Account except for the possibility to open or close the latter.

Beneficiary

Refers to a legal or natural person, recipient of a Payment Transaction issued by the Customer.

Card

Refers to a payment card with systematic authorisation linked to the Payment Account, issued in the name of the Customer and, when applicable, the Cardholder.

Customer

Refers to a natural or legal person acting in the course of their professional activity and in whose name one or more Payment Accounts are opened in the website and registered with PECUNIA CARDS EDE, S.L.U.

Accountant

Refers to a natural person retained by the Customer, who holds restricted rights to the Payment Account(s). Such person may in particular consult the balance of the Account(s), sort, export, modify the transactions (add receipts, complete VAT, etc.) and connect accounting tools to the Personal Area.

The accountant cannot manage the parameters of the Cards, the Accounts cannot hold a Card.

Payment account(s) or Account(s)

Refers to the Principal Payment Account and/or the Additional Payment Accounts opened in the Institution's on behalf of the Customer for the purpose of providing the Payment Services.

Additional Payment Account(s)

Refers to the Payment Account(s) created by the Customer in addition to the Principal Payment Account, in the Institution’s, in order to provide Payment Services and manage cash more effectively. This feature is only offered to Customers who have subscribed to a FREELANCER, BUSINESS or ENTERPRISE package.

Principal Payment Account

Refers to the payment account opened in the Institution, on behalf of the Client, to provide Payment Services. This account is identified as a principal account, on which the Institution invoices Payment Services.

Framework Payment Services Contract or Contract

Refers to this Contract made of the General Conditions of Use, special conditions and appendices.

Identification data

Refers to the combination of a login and a password, specific to a User, allowing access to the Personal Area.

Personalised security data

Refers to the personalised data provided to a User by the Institution for authentication purposes. Personalised Security Data includes Credentials, as well as any data related to a Simple Authentication or Strong Authentication procedure defined by the Institutions.

Issuer

Refers to the Institution issuing the Card to the Customer for a fee.

Employees

Refers to all of the employees under the responsibility of an Administrator.

Personal area

Refers to the dedicated environment of the Customer (or a customer-designated User) accessible via the Website or Application or the Site using the Identification Data.

Business day

Refers to a calendar day corresponding to the operating hours of the Customer Service as indicated on the website or the Application.

Working day

Refers to a calendar day with the exception of Saturdays, Sundays, and public holidays in Spain during which the payment infrastructures and banks exercise their activities in regular operation.

Employees

Refers to a natural person, mandated by the Customer, or added by the Administrator, who has restricted rights to the Account. He/she can make purchases by Card.

Password

Designates the secret code to access the Personal Area.

Payment order

Refers to the payment instructions ordered by the Customer in accordance with the procedure set out in the Contract to execute a Payment Transaction.

Payment transaction

Refers to a withdrawal or transfer of funds action executed by the Institution and charged to the Payment Account.

Payer

Refers to a legal or natural person who holds the Payment Account(s) and authorises a Payment Order from that Account.

Cardholder

Refers to a natural person mandated by the Customer to use a Card in the strict context of the Customer's professional activity.

Account information services provider

Refers to an authorised or registered Payment service provider that is distinct from the Institution and, with the consent of the Customer, can access their Account(s).

Card scheme

Refers to the Mastercard/Visa payment processing network.

Payment services

Refers to the payment services provided by the Institution under the Contract. PECUNIA CARDS EDE, S.L.U. (the “Electronic Money Entity”), a Spanish company with registered office at Calle Guzmán El Bueno, number 133, Edificio América, Bajo B, 28003 Madrid, provided with NIF: B-86972346, and is registered in the “Registro Mercantil de Madrid”. The Electronic Money Entity is subject to the supervision of the Bank of Spain and is registered in the “Registro de Entidades de Dinero Electrónico del Banco de España” under the number 6707.

Services

Refers to all services provided by the Institution to the Customer under this Contract, including the Payment Services.

Customer service

Refers to the customer support whose contact details are available in article 13 of the General Conditions.

Website

Refers to the website published and operated by the Institution to access the Personal Area.

Owner

Refers to a natural person, mandated by the Customer, having all the rights on the Account(s) including creating and closing it/them.

User

Refers to a natural person expressly mandated by the Customer to access the Customer's Personal Area and use the Services, within the limits defined by the Customer. Owners Administrators, Managers, Members and the Accountant are Users under a duly completed power of attorney or representation.

TiC

Refers to the brand under which the Institution markets the Services.

2.Object

The purpose of this Contract is to provide a framework for the provision of the Services to the Customer, in consideration of the fee payment determined in Article 2 of Title 1.

Services provided by the Institution include:

a. Holding one or more Payment Accounts,

b.Issuing Cards,

c.Execution of the following Payment Transactions associated with the Payment Account(s) by:

c.1. Cards

c.2. Transfers

c.3. Qr

c.4. SMS

Title 1 of these Terms of Use contains the general provisions relating to the offer of the Institutions. Title 2 details the Payment Services associated with the Account(s) provided by the Institutions, excluding Card Payment Services. Title 3 details the conditions of subscription, operation and use of the Card.

The Contract consists of these General Conditions of Use, the Special Conditions, and the following Appendices:

Appendix 1: **Documents required to open a Payment Account**

Appendix 2: **Rights associated with each User**

Appendix 3: **Special operations**

Use of services

Services are provided to the Customer through their authorised Users, whose rights depend on the profile assigned to them. Profiles are detailed in Appendix 2 – Rights associated with each User.

The Customer, through its Owner, expressly undertakes to act in accordance with the terms of the Payment Services Framework Contract.

The Owner undertakes to inform Users of the terms and conditions of the Payment Services Framework Contract.

Title 1. General provisions

1. **Underwriting conditions**

The Customer guarantees to be acting in their professional capacity and declares to be registered in one of the following states: Austria, Belgium, Bulgaria, Cyprus, Croatia, Denmark, Estonia, Finland, France, Greece, Hungary, Ireland, Iceland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Norway, Netherlands, Poland, Portugal, Slovakia, Slovenia, Czech Republic, Federal Republic of Germany, Romania, Sweden.

The Customer expressly warrants that they own one of the legal forms listed at the following.

Spain:

- Sociedad anónima,
- Sociedad limitada,
- Sociedad colectiva,
- Sociedad comanditaria.

Sweden

- Limited company,
- Limited partnership,
- Trading partnership,
- Sole trader,
- Economic association.

Denmark:

- Danish Private Limited Company
- Danish Private Limited Company
- Danish General Partnership
- Danish Limited Partnership
- Danish Sole Proprietorship

United Kingdom

- Private company limited by shares (LTD);
- Company limited by guarantee;
- Unlimited company (UNLTD);
- Limited Liability Partnership (LLP);
- Community Interest Company;
- Industrial and Provident Society (IPS),
- Royal Charter (RC).

Estonia

- Private limited company (OÜ)
- Public limited company (AS)
- General partnership (TÜ)
- Limited partnership (UÜ)
- Commercial association (ühistu)

Legal or natural persons exercising an activity in the sectors listed at the following address are not authorized to open a Payment Account with TiC:

LIST of **Prohibited activities**

Legal or natural persons performing an activity in the sectors listed below are not authorized to open a Payment Account:

- Sex (pornography, sex toys, escorting, prostitution)
- Weapons, war vehicles including copies
- Tobacco (including THC/cannabidiol)
- Casino, gambling
- Cryptocurrency (trading, exchanges, investments, mining)
- Fortune telling, astrology
- Trading platforms (currencies, precious metals, gems, other commodities, securities)
- Unlicenced payment services (crowdfunding, crowdlending, marketplace)
- Online selling of chemical products, nutra and drugs of any kind
- Selling of goods/services that may result in harming honor or reputation of others
- Religious associations
- All illegal activities
- Trading, trading and mining or any investment in digital assets if not registered with a regulatory authority
- Insurance brokerage activity if not registered with an administration

2.Pricing conditions

Services are provided to the Customer in return for payment of the fees detailed at the following addresses:

payment services

Special operations

The fees are billed to the Customer by debiting its Principal Payment Account and, in the absence of a sufficient provision, on one of the Additional Payment Accounts if due.

If no provision has been recorded for the total amount due in the Principal Payment Account or one of the Additional Payment Accounts when payment is due, charges may be partially debited ("Partial Charges") in the amount of the available balance of the Principal Payment Account or of one of the Additional Payment Accounts.

A receipt is then issued summarising the charges debited and the outstanding balance for payment, which can be accessed via the Personal Area.

These Partial Charges are debited in priority before the execution of any Payment Order from the Customer Accounts.

3.Blocking of the Personal Area

The Institution reserves the right to block access to the Personal Area, for reasons related to security or in case of presumption of an unauthorized or fraudulent use of the Personal Area, or any data related to the Personal Area.

In case of blockage, the Institution informs the Customer by any means and communicates the reasons for this blocking, unless security concerns or legal prohibitions justify the non-disclosure of these reasons.

Access to the Personal Area will be restored as soon as the reasons justifying the blockage have disappeared. The Customer may at any time request to unblock its Personal Area by contacting the Institution by email or by telephone, at the contact information indicated.

To restore the access to the Personal Area, the Institution may require new Identification Data for all Users.

In addition, the Customer is invited to change the Password of their Personal Area periodically and whenever there is suspicion of use by a third party.

4.Duration

The Contract is concluded for an indefinite period of time from its online acceptance by the Parties.

This Contract is subject to:

The validation of the money laundering and financing of terrorism process of identification.

If this condition is not realized within a period of six (3) months from the date of signature of the Contract, the Institution reserves the right to terminate the Contract immediately, without the need to notify its resolution decision.

5.Amendment

Any significant amendment to this Contract adverse to the interests of the Customer will be communicated to the Customer sixty (60) days prior to the date of application. The absence of dispute during this period will be worth acceptance of the amendment brought to the Contract. If the Customer refuses the proposed changes, it must notify the termination of the Contract before the expiry of the aforementioned period. The termination will take effect at the date of application of the amendment.

Any amendment of this Contract by the Institution in response to legal and regulatory measures will take effect upon their entry into force.

Any new services offered by the Institution will be subject to an amendment of the Contract.

6.Transfer

The Institution reserves the right to transfer this Contract to any entity of the group, controlled, controlling, or under common control with the Institution, upon prior written notification sent to the Client. If there is no objection from the Customer within thirty (30) days of written notification, the Contract will be transferred with effect at the end of this 30-day period.

7.Termination

7.1. Termination of right

7.1.1 Termination by the Customer

The Customer may at any time request the termination of this Contract, unless they have subscribed to an annual subscription.

The cancellation request can be made by the account Owner per email to the address support@tic.business and will take effect at the expiry of a period of notice of thirty (30) days from the date of receipt by the Institution of the Application ("Effective Date").

In the event of an annual subscription, during the first year, the request for termination of the Contract can be made thirty (30) days prior to the anniversary date of the Contract. At the end of

the annual commitment period, the Customer may request a termination at any time, provided that the notice period of thirty (30) days is respected.

In order to ensure the payment of sums due by the Customer and to guarantee the successful completion of Payment Transactions, the Customer must maintain a sufficient balance on their Principal Payment Account.

7.1.2. Termination by the Institutions

The Institution may also automatically terminate the Contract, by email notification, with a thirty (30) day notice period. In this case, the Institution will send a notification to the Customer and, where applicable, to the Cardholder. The institution's obligation to comply with a notice is not applicable if it suspects the Cardholder or a third party of misusing or fraudulently using the Card.

7.2. Termination for breach by either of the Parties

In the event of a Party's serious breach of its obligations under this Contract, the other Party may terminate the Contract with immediate effect from receipt of an email notification sent to the contact address of the breaching Party ("Effective date").

Serious breach of the Customer includes but is not limited to: Non-payment, carrying out an illegal or prohibited activity as defined in Article 1, threatening the company’s staff, communicating false information or refusing communication, upholding a Payment account with excessive or persistent negative balance, suspicion of fraud.

The Institution may also terminate the Contract immediately and by right for any reason related to a risk or suspicion of money laundering and/or terrorist financing, without justification, in accordance with the regulations in force.

7.3. Collective proceedings

In case of collective proceedings of a Party, the Contract may be solved by letter with acknowledgment of receipt to the other Party under the conditions and within the time limits fixed by law and according to the decision of the appointed representative or liquidator.

By collective procedure, it is understood: the appointment of an ad hoc agent, a judicial administrator, the opening of reorganization or liquidation proceedings, or the loss of the licence of the Institution.

7.4. Death of the physical person

In the event of the death of the physical person Customer, confirmed by an official document, the Institution will block the Payment Account(s), then close the Account(s), subject to the settlement of the current Payment Transactions initiated prior to the death and the payment of charging fees on the available balance of the Principal Payment Account, or if its balance is not sufficient, on the available balance of Additional Payment Accounts. The Account(s) may be debited for certain Payment Transactions subsequent to the death of the Customer at the request of the notary or the Heirs, under certain conditions.

At the end of the registration in the Payment Account(s) of all related Payment Transactions, the Institution will give the notary or the Heirs the total amount of the credit balance of the Account(s).

7.5. Effects of termination of the Contract

The Payment Account(s) will be closed on the Effective Date, provided that the Customer has paid all amounts due under this Contract. The termination of the Contract does not affect the services previously performed or being executed on the Effective Date. Payment Transactions initiated before the Effective Date will not be called into question by the termination and will be executed in accordance with the provisions of the Contract.

The Institution reserves the right to maintain the Payment Account(s) for a period of twelve (12) months in order to cover any subsequent disputes and claims by Payers or to enable the liquidation of any on-going transactions.

During this period, the expenses detailed in 2 “Pricing Conditions”, including subscription fees, will remain applicable to the Payment Account(s) maintained.

As part of the closure of the Account(s), the Institution will transfer the total balance of the Payment Account(s) to the payment or bank account in the SEPA zone designated by the Customer.

As from the notification of cancellation of the Contract, the Customer must send the Institution the bank details (IBAN) of the SEPA zone bank or payment account required for the transfer of the balance held on the Payment Account(s).

During this period and until the transfer of the total balance of the Payment Account(s), the Institution continues to deduct the costs detailed in 2 “Pricing Conditions”, including subscription costs. These costs are applicable to the Payment Account(s) and are related to the continuing operation of the Payment Account(s).

8. Liability and Force majeure

8.1. Liability

The Institution is absolutely unconcerned by the legal and commercial relations and any litigation between the Customer and a Payor or the Customer and a Beneficiary.

The liability of the Institution is limited to the compensation of direct damages. Thus, the Institution's liability cannot be incurred in the event of indirect damages (such as financial losses, loss of income, loss of customers, damage to the image, moral damage, etc.) that could result from the use of the Services. In addition, the Institution cannot be held responsible for any damage resulting from the implementation of legal and regulatory obligations incumbent upon it (example: asset freezing measure, blocking of a Payment transaction for reasons of fight against money laundering and terrorist financing, etc.).

8.2. Force majeure

The Parties will not be held responsible for any delay or non-performance that is related to a case of force majeure. "Force majeure" means any exceptional event beyond the control of the Parties which cannot be reasonably foreseen at the time of the conclusion of the Contract and the effects of which prevent fulfilment of the obligations arising from these.

The Parties have a period of thirty (30) days to remedy the case of temporary force majeure. After this period, each Party may terminate the Contract by letter with acknowledgment of receipt. The effective date taken into consideration will be the receipt of the letter.

If the case of force majeure is final, this Contract is resolved and the Parties released from their obligations.

9. Availability of Services

The Institution undertakes to make its best efforts to ensure that the Services are accessible 24 hours a day and 7 days a week. However, access to the Personal Area may be temporarily unavailable for technical reasons. The Institution declines all responsibility, including but not limited to:

a. Interruption of the Application for technical maintenance operations or updating published information.

b. In the event of temporary inability to access the Application (and / or the websites and applications linked to it) due to technical problems and regardless of their origin and provenance.

c. Unavailability, overload, or any other cause preventing normal operation of the mobile network used to access the Application.

d. Contamination by possible computer viruses circulating on the network.

e. Any direct or indirect damage caused to the Customer, whatever its nature, resulting from the access, or the use of the Application (and / or sites or applications linked to it).

f. Abnormal use or unlawful exploitation of the Application.

g. Loss by the Customer of his username and / or password or in case of usurpation of his identity.

10. Personal data

The processing of personal data (hereinafter the "Personal Data") is governed by this contract, its annexes and TiC's Data Protection Policy available at the following address:

Link here

By accepting this Contract, the Customer authorizes the Institution to communicate his/her Personal Data to partners or subcontractors whose activity has been outsourced to them for the performance of the Services.

11. Professional secrecy

The Institution is bound by professional secrecy. Professional secrecy may be waived by virtue of a legal, regulatory or prudential obligation. In addition, the Institution may be required to transmit data subject to professional secrecy to contractors and subcontractors contractually linked with the Institution in order to provide essential operational tasks within the framework of access to all payment Services.

In addition, the Customer may authorize the Institution to waive professional secrecy with regard to third parties by indicating them. Third parties receiving information covered by professional secrecy are required to keep them strictly confidential.

12. Evidence agreement

In the context of this Contract, the Parties intend to establish the rules relating to admissible evidence in connection with the execution of the Services. For this purpose, the Customer and the Institution recognize that the proof of Payment Orders transmitted after Simple Authentication or Strong Authentication may be reported by the reproduction on computer media of the Authentication registered by the Institution. Unless proven otherwise by the Customer, the items held by the Institution shall prevail.

The Institution may be required to certify the execution dates of Payment Transactions on the Account by a time stamping process. This process will be a proof of the data it contains.

The Customer hereby agrees to the recording of all electronic communications made possible with the Institution for purposes of proof and improvement of the Services.

13. Communication and Customer Service

The Customer may contact the Customer Service Department of the Institution:

By Email at support@tic.business

By phone: +34 910 606 677

By mail: TiC Global Payments, Avd. General López Domínguez Ed. Puerto Azul Portal 2A, entreplanta oficina 1 (Marbella) Málaga Spain

Via the Support Website Chat

Regarding the sending of complaints, the procedure is specified in the “Claims Processing” article of this contract.

14. Language

The language applicable to contractual relations is English.

15. Claims processing

The Customer is invited to contact the Claims Service (support@tic.business) for any claim relating to the execution of the Contract.

The Customer agrees that the Institution responds to their claims in a durable medium.

The reply will be sent as soon as possible and at the latest within fifteen (15) Working Days following receipt of the complaint by the Institution. However, for reasons beyond its control, the Institution may be unable to respond within this fifteen (15) day period. In this case, it will communicate to the Customer a response specifying the reasons for this additional delay and the date on which it will send the definitive answer. In any case, the Customer will receive a definitive answer no later than thirty-five (35) Business Days following receipt of the complaint.

In case of dispute, the Institution will inform the Customer about the existence or not of an appropriate dispute resolution body.

16. Non-transferability

This Contract may not be transferred in whole or in part by the Customer. The Customer may be held liable for any breach of this provision and the Institution may terminate the Contract without delay.

17. Independence of stipulations

The invalidity or invalidity of one or more terms of the Contract does not affect the validity of the Contract or the other stipulations of the Contract. As a result, the Contract and other clauses will remain in effect.

18. Applicable law and competent courts

The law applicable to the Contract is Spanish law. Any dispute relating to the formation, validity, interpretation, performance or breach of the Contract falls within the exclusive jurisdiction of the Spanish courts, including in the event of a warranty claim or plurality defendants.

Title 2. Specific provisions applicable to the Account(s) and the related Payment Services

1. How the Payment Account(s) work(s)

In the event of acceptance of the opening of the Principal Payment Account, an email of confirmation will be sent by the Institution to the Customer. The payment account number (IBAN number) opened in the name of the Customer is available in its Personal Area.

The Customer can then send funds to their Principal Payment Account by a first incoming transfer from an account opened in their name with a payment service provider located in the European Union, the European Area or a third countries imposing equivalent obligations in the fight against money laundering and the financing of terrorism. The Customer may then create Additional Payment Accounts (subject to validation by the Institution of the Know Your Customer, order Cards and add Users to the Account(s), in accordance with the conditions of use of the Card provided for in Title 3. Notwithstanding the foregoing, the Customer may not make any Payment Transactions until the Institution has proceeded activation of all Services.

a. Designation of Users

The opening of an Account is made through the Owner/Representative who has the rights to represent and engage the Customer. The Owner/Representative may be a corporate officer or a natural person other than the corporate officer expressly mandated by the Customer. In the event of loss by the Owner of their rights to their Account(s) (for example, change of the corporate officer or revocation of the Power of attorney of the authorized person), the Customer undertakes to inform the Institution without delay. In the absence of notification or in the event of late notification, the liability of the Institution cannot be engaged.

Moreover, the Customer may give Power of attorney or representation to Administrators or Members authorized to use the Services on their behalf and for their account, and under their entire responsibility. The power of attorney or representation will only take effect upon receipt by the Institution. The power of attorney or representation ceases automatically upon the death of the Owner or the Administrator who has issued it. The power of attorney or representation may be revoked by the Customer at any time by informing the Institution through the support email without undue delay. If the notification is not made or is made late, the Power of attorney remains valid and the Institution cannot be held liable. The Customer expressly discloses the obligation of professional secrecy relating to the Payment Account data in respect of Users.

The Customer will add each User the pre-set scope of the rights he/she has on the Payment Account(s). Each User is assigned Personalized Security Data of his/her own, in order to access his/her Personal Area. The Personal Area of each User is personalized according to the rights granted to him/her by the Customer. The different Users profiles are: Owner/Representative

(Admin), Employee and Accountant. The rights associated with each User are detailed in Appendix 2.

b. Personalized security data

The Customer must take all reasonable steps to maintain the confidentiality and security of its Personalized Security Data. It also undertakes to make users aware of the

preservation of the confidentiality and security of their own personalized security data.

The Customer (and each User) undertakes not to communicate their Personalized Security Data to third parties. Exceptionally, the Customer may communicate them to an Access Service Provider for the purpose of providing the account information service or the payment initiation service. In this case, and having expressly consented to access their Account, the Customer must ensure that the said Provider is approved or registered for the aforementioned services, and that they enter their Personalized Security Data in a secure environment.

The Institution reserves the right to refuse access to a Payment Account to such a Provider if it suspects that access to this Account is not authorized or fraudulent. The Institution will inform the Customer by any means of the refusal of access to this Payment Account and the reasons for such refusal, unless this information is not available for objectively justified security reasons or under a relevant provision of national or European Union regulation.

c. Statements

The Customer is informed by the Institution of any provision of information on a durable medium within the meaning of the law and case law.

The Institution provides the Customer with a statement of the Payment Transactions related to each one of their Accounts. This(ese) statement(s) is(are) available in their Personal Area.

The Customer undertakes to check the contents of the Statement(s) of Operations and to keep it for a minimum of five (5) years. The statement(s) is(are) a legal record of all Payment Transactions made on every Payment Account.

d. Balance of the Payment Account(s)

d.a. Payment Account(s) with a negative balance

As the Customer's Payment Account balance cannot be in any way negative, the Customer undertakes to maintain a sufficient balance on each Payment Account to ensure the execution of the Payment Transactions. In the case of an insufficient balance on a Payment account, the Institution shall reject the Transactions concerned.

d.b Payment Account(s) with a positive balance

The positive balance of the Customer Payment Account(s) may, if above a certain level, generate additional costs for the Institutional linked to the operation of such Account(s).

Above a certain balance held on their Account(s), the Institution reserves the right to invoice additional charges to Customers.

e. Inactive account(s)

A Customer's Payment Account is considered inactive when, after a period of twelve (12) months, it has not been the subject of any transaction (excluding management fees) on the initiative of the Customer (or any User) and that then latter has not made any representations to the Institution in any form whatsoever.

When an Account is considered inactive, the Institution informs the Customer by any means. In the absence of a response from the Customer or any new transaction on this Account and in the case where the balance is positive, the Account will be closed at the end of a period of ten (10) years from the last transaction on the account. The Customer will be informed by any means six (6) months before the effective closing of the Account.

f. Fight against money laundering and terrorist financing

As an EMI, the Institution is subject to the legal and regulatory provisions relating to the fight against money laundering and the financing of terrorism. For this purpose, the Institution must carry out all the necessary procedures relating to the identification of the Customer and, when applicable, the ultimate beneficial owner, as well as to the verification of the identity of the latter. Throughout the duration of the Contract, the Customer undertakes to keep the Institution informed about any changes without delay concerning, in particular, their activity, the identification of their corporate officers and beneficial owners, including a change of control.

In addition, the Institution must inquire about the origin of the Payment Transactions, their purpose and the destination of the funds. From an operational point of view, the institution is required to set up a system for monitoring and detecting atypical payment transactions.

The Customer undertakes to comply with obligations to combat money laundering and terrorist financing by providing information to the Institution about any unusual Payment Transactions detected by the Institution.

The Institution reserves the right to request any other document or additional information if deemed necessary to meet its vigilance obligations in the sense of the fight against money laundering and the financing of terrorism. As such, the Institution could postpone the opening of the Payment Account or temporarily block and even close this Payment Account and/or all other Customer's Accounts in case of persistent suspicion.

In addition, the Customer is informed that the Institution may be required to report any suspicion of money laundering or terrorist financing.

By accepting this Contract, the Customer is informed that no proceedings for breach of professional secrecy may be brought against the Institution in the exercise of its obligation to declare suspicion.

g. Protection of funds

Institution states that the deposited funds will be safeguarded in accordance with the legal requirements specified in article 21.1 a) of Royal Decree-Law 19/2018, of November 23, on payment services and other urgent financial measures.

Institution expressly declares and undertakes that said funds will not be mixed at any time with the funds of any other natural or legal person who are not clients of the payment services on whose behalf such funds are made available.

4. Execution of payment transactions: general rules

a. Payment transaction

A Payment Transaction is independent of the underlying civil or commercial obligation between the Customer and the Payment Recipient. The Institution therefore remains foreign to any civil or commercial dispute that may arise between the Customer and the Beneficiary.

A Payment Transaction may be initiated by the Customer who gives a Payment Order (transfer) directly, by the Customer who gives a Payment Order through the Beneficiary (card) or by the Beneficiary (direct debit).

b. Security of payment instruments

The Customer will take reasonable steps to maintain the security of their Custom Security Data. Upon knowledge of loss, theft, misappropriation or any unauthorized use of a payment instrument or related data, the Customer shall promptly inform the Institution for the purpose of blocking (or opposition) of the instrument, by email or by phone (contacts indicated in article 13).

If the blocking request was made by telephone, the Customer must confirm his request in writing (postal or electronic mail). The Institution reserves the right to subsequently request a receipt or a copy of the complaint following the theft or fraudulent use of its Account. The Customer undertakes to respond to the Institution's request as soon as possible.

The Institution executes the request for opposition as soon as it receives it. The event will be recorded and timestamped. An opposition number with timestamp will be communicated to the Customer. A written confirmation of this opposition will be sent to the concerned Customer by email or in their Personal account.

In case of suspicion of fraud, proven fraud or security threats, the Institution will inform Customer according to a secure procedure that will be communicated to them.

c. Strong authentication

In accordance with the law, the Institution applies Strong Customer Authentication when it:

1. Accesses the Customer’s Online Payment Account(s);
2. initiates an Electronic Payment Transaction (except in the event of transfer to another account held in the name of the Customer);

Strong Authentication is performed by the input of a 2-factor authentication code

received by SMS on the phone number associated with the User, in the dedicated field of the Application.

5. Issuing Cards

The Institution issues physical and virtual Cards in the conditions detailed in Title 3.

6. Execution of Payment orders by transfer

a. General description

The Customer may issue, via a User who has the necessary rights (Owner or Administrator) a payment Order by transfer from their Payment Account to an account opened in the books of another payment service provider.

The Customer may initiate Transfer Orders in Euros.

To initiate a Transfer Order, the User who has the necessary rights connects to his/her Personal Area using his/her Identification Data, entering:

- The Payment account where the Customer intends to initiate the Payment Operation;
- The amount of the Payment Transaction (the User must ensure that the selected Account has a balance sufficient to cover the amount of the Payment Transaction and any associated costs);
- The identity of the Beneficiary of the transfer as well as his/her bank details (IBAN);
- The reason for payment.

The User is invited to check all of this information before validating his/her Transfer Order. The consent of the User to the Transfer Order is collected according to the procedure indicated in the Personal Area. The User must follow any strong authentication procedure requested by the Institution. The Transfer Order is irrevocable once it has been definitively validated by the User from his/her Personal Area. The Institution will not accept any request for cancellation of a transfer beyond its date of irrevocability.

Transfer Orders are time stamped and kept for the applicable legal period.

When the consent is given through a Service Provider providing a payment initiation service, the form of this consent is determined by the Customer and the said Provider, under the conditions agreed between them. The Institution is not a party to these conditions and does not have to verify the Customer's consent.

When the Transfer Order is initiated, at the request of the Customer, by a service provider providing a payment initiation service, the Customer may not revoke the Order after granting consent.

b.Transfers denominated in Euros

The Transfer Order must comply with SEPA rules set forth in the “SEPA Credit Transfer Rulebook.”

For the standard Transfer Orders, they will be executed at the latest at the end of the day indicated by the Customer. If it is not a Business Day, the Institution will execute the Transfer Order on the next Business Day.

c. Refusal of execution

The Institution may refuse to execute any incomplete or incorrect Transfer Order. The Customer will then be asked to re-issue the Order to edit missing or incomplete information.

In addition, the Institution may suspend a Transfer Order in the event of serious doubt of fraudulent use of the Account, unauthorized use of the Account, breach of security of the Account, suspicion of money laundering / financing of terrorism, or in the event of an assets-freeze order issued by an administrative authority.

In case of refusal of execution or blocking of a Transfer Order, the Institution will inform the Customer by any means as soon as possible, and at the latest by the end of the first Business Day following the Date of receipt. If possible, the Institution will indicate the reasons for the refusal or blocking to the Customer, unless prohibited by a relevant provision of national or European Union law. The Customer is informed that such notification may be subject to the charges indicated in the Pricing (Article 2 of Title 1 2) if the refusal is objectively motivated.

d. Contestations concerning Payment Orders by Transfer

If the Customer wishes to contest an allegedly unauthorized or incorrectly executed Transfer, they must contact the Institution's customer service by phone call or email as soon as possible after becoming aware of the discrepancy and no later than four (4) weeks following the registration of the Payment Transaction in the Account.

The institutions will be exempt from liability with respect to Payment orders, even being against the will of the payer, have been obtained as a result of an order received by the institution for whose authentication the established security requirements have been met.

The use of the PIN by a person other than the HOLDER presupposes gross negligence or, fraud on the part of the HOLDER.

The institutions without prejudice to adopting the measures it deems pertinent, is exempt from liability in case of lack of attention to your card by any of the businesses, banks and savings banks committed to the sale of goods or provision of services, or for incidents of a technical or operational nature in ATMs.

The institutions will also be exempt from liability regardless of the incidents and responsibilities that may arise from the operation carried out between the establishment and the CARD HOLDER.

The institutions exclude, from the scope of its application, Visa's Zero Liability Policy (Visa Global Zero Liability Policy), submitting to current European regulations on the matter.

The system of liability of the ordering party in the event of unauthorised payment transactions, which, in each case, regulates the applicable legislation on the matter, shall apply. Specifically, the HOLDER who does not hold the status of consumer or micro-enterprise in the terms established in Royal Decree-Law 19/2018, of November 23, on payment services and other urgent measures in financial matters, will be obliged to bear the losses derived from unauthorised payment operations resulting from the use of the lost, stolen or improperly appropriated payment instrument by a third party, as long as the loss, theft or misappropriation of the payment instrument is not reported to the institutions.

Lastly, the institutions accounts may only deposit a balance in euros. In no case, it will be possible to deposit Cryptocurrencies, leaving the institutions exempt from any type of responsibility related to them.

The Institution cannot be held liable when the incorrect execution of the payment Transaction is the result of an error by the Customer on the Unique Beneficiary Identifier (IBAN). The Institution will endeavour to recover funds committed to the payment Transaction.

e. Receiving Transfers

Under the terms hereof, the Customer expressly mandates the Institution to receive SEPA Transfer Orders in Euros from an account opened in the books of a payment service provider located in the SEPA zone in their name and on their behalf.

The Institution credits one of the Customer's Payment Accounts not later than four business days on which their own account has been credited with the funds. As soon as the transaction is credited to the Customer's Payment Account, the Institution shall make a summary of the transaction including the following information available in the Personal Area: amount, date and time, Payment Transaction number, name of the Payer, debited account and reason of the Transaction (if applicable).

Title 3. Terms of Use Specific to Card Payments

This title relates to the Professional Card and defines the conditions of subscription, operation, and use of the Card by the Cardholder. The conditions of this Title remain applicable under the same conditions except modifications made by the Issuer notified to the Cardholder and to the Customer within thirty (30) days' notice period.

The Card is a payment card with systematic authorizations associated with the Payment Account(s) opened in the name of the Customer. The Card is for professional use only. The Card can be used for proximity payments (EPT, NFC), cash withdrawals from ATMs (ATMs) and remote Card Payment Transactions (RCPT).

1. Obligations of the Cardholder

After having read and accepted these general conditions of use of the Card, the Owner undertakes, under his/her full responsibility, to bring them to the attention of the Cardholder and to ensure that they are respected. The Owner is invited to keep them in a durable medium accessible to the Cardholder.

2. Designation of a Cardholder

The Customer may order, through the Personal Area of a User who has the necessary rights (Owner or Administrator), Payment Cards in order to assign them to the Cardholders that has designated.

Cards issued by the Institution are physical or virtual Mastercard/Visa payment cards with systematic authorization. The Cards are attached to a Customer's Payment Account and are issued in exchange for the payment of fees detailed in Article 2 of Title 1. These fees are charged to the Customer's Principal Payment Account in accordance with the provisions of the Contract.

The Customer undertakes to transmit all information relating to the Cardholder required by the Issuer in order to issue a Card in the name of the latter acting on behalf of the Customer.

When the Customer designates a Cardholder, he/she will be invited to create his/her Personal Area, with his/her own Identification Data. The Cardholder must transmit the information and documents requested by the Institution through his/her Personal Area. The Institution reserves the right to discontinue the use of the Card. If necessary, the Customer is informed of the reason for the refusal, unless national or European legislation prevents the communication of this information.

The User who has the necessary rights on the Account has the option to set up for each Card ceilings of expenditure, within the limits of the ceilings imposed by the Institution.

3. Card issuance

3.1. Physical card

The Institution sends the physical card by mail to the Customer's address. For reasons of security and confidentiality, the Cardholder pre-determines a PIN code in his/her Personal Area. The Cardholder is prompted to activate the Card in accordance with the instructions provided by the Issuer included in the mail.

Upon receipt of the Card, the Cardholder must provide a signature on the area provided for this purpose. The Cardholder is prohibited from affixing any other physical or functional alteration on the Card.

3.2. Virtual card

The virtual card is accessible directly from the Personal Area of the Cardholder. For security reasons, strong authentication is necessary to reveal the information allowing its use (PAN, CVV, expiration date).

4. Card operations

4.1. General provisions

The Card is exclusively issued for business expenses. The Cardholder commits not to use the Card for personal purposes or on behalf of a third-party other than the Customer. It is strictly prohibited to lend the Card to a third-party.

The Card is a payment card with systematic authorization. Therefore, prior to any effective execution of a Payment Transaction, the Payment Account balance is verified by a request for authorization. If the authorization is not obtained by the Beneficiary, the Card Payment Transaction will be refused. The Payment Transaction may also be refused by the Issuer in case of suspicion of fraud by the Cardholder or a third-party.

The Cardholder may use the Card within the limit of the balance available on the related Payment Account and the ceilings defined by the Customer. The Customer remains responsible for all Card Payment Transactions made on this Account.

The Customer agrees to fund every Payment Account to enable the execution of the Card Payment Transactions made by the Cardholder.

The Cardholder can make payments in euros as well as in foreign currencies under the conditions described below.

4.2. Payment transaction in currency according to the Scheme rules

The Card issued by the Issuer operates as an international payment card, allowing currency exchanges by the Card Scheme. Card Payment Transactions may be given in any currency

defined by the Card Scheme, according to the specific conditions of the Card Scheme. The exchange rate that may be applicable is that in effect on the date of the Card Scheme's processing of the Transaction.

4.3. Personalized security data

The Card is a payment instrument with Personalized Security Data. The Authentication procedure will be different depending on whether the Cardholder conducts a remote payment or a proximity payment. The Cardholder undertakes to follow any authentication procedure each time he/she receives the instruction.

4.4. Using Personalized Security Data for Proximity Payment and Cash Withdrawal

The PIN code of the Card is strictly personal and confidential. The Cardholder must take all necessary measures to ensure the confidentiality, which is intrinsically linked to the security of the Card. For this purpose, the Cardholder is invited to never communicate this confidential code to an unauthorized third-party. The Cardholder is reminded that merchants, e-commerce sites, the Customer, the Issuer, representatives and any other partners are not authorized to request this PIN code. In this case, the Cardholder must refuse to transmit this code.

The Cardholder must never write the PIN code on the Card or any other medium. If the Cardholder forgets the PIN code, he/she can check it on their personal area.

To make a proximity payment or a cash withdrawal, the Cardholder must verify that the Electronic Payment Terminal (EPT) or the ATM displays the logo of the Card Scheme. At the time of entering the PIN code, the Cardholder must perform this action discreetly to prevent any capture of confidential data by a third-party. In order to prevent any fraudulent use of the Card, the entry of the PIN code is only possible within the limits of three successive entries. At the end of a third unsuccessful attempt, the Card is blocked or retracted by the ATM. The Cardholder is invited to contact Customer Service to obtain a new Card.

4.5. Using Personalized security data in remote payments

The Cardholder may issue Remote Card Payment Transactions. For this purpose, he/she will be asked to provide the following Personalized Security Data: the Card number, the validity date and the CVV on the back of the Card. For each new Payment Transaction, and depending on the case, the Cardholder must also communicate a single-use authentication code received by SMS in order to validate the payment.

Any Card Payment Transaction made from abroad may result in the additional charges to be paid by the Customer for sending the single-use authentication code by SMS.

5. Consent and irrevocability of the Payment Transaction

The Cardholder's consent for the execution of the Payment Transaction is given differently depending on whether payment is made remotely (RCPT), for proximity payments (EPT, NFC) or for withdrawals of cash in ATMs (ATMs).

Remote Card Payment Transactions: Consent is provided by the communication of Personalized Security Data related to Remote Use (Card Data and One-Time Authentication Code) and being a Strong Authentication of the Cardholder.

Proximity payments: Consent is given either by entering the confidential code (PIN code) once the Card is introduced in the EPT (Electronic Payment Terminal), or by the use of contactless payment on a EPT within the legal limit in force.

Cash withdrawals: Consent given by entering the confidential code (PIN code) on the keypad of an ATM.

Any Card Payment Operation authorized by the Cardholder in one of the forms described above is irrevocable.

6. Receiving and executing the Card Payment Transaction

The Parties agree that a Card Payment Transaction is deemed to be received by the Issuer at the time this Order is communicated to it by the Beneficiary's payment service provider, or by the ATM manager through the clearing system. When the Card Payment Order is executed within the European Economic Area, the Issuer will transfer the funds to the Beneficiary's payment service provider within one Business Day.

The Customer is informed that Cash Withdrawal Orders are executed immediately by making cash available to the Cardholder.

7. Cardholder's Personal Area

The Cardholder owns a Personal Area accessible via the mobile application or the website using the identification data. Through his/her Personal Area, the Cardholder has the following features: view of information related to his credit card, details of transactions made with the Card.

8. Liability and obligations of the Cardholder

The Card is a payment instrument intended for professional use. Consequently, the Cardholder agrees to use the Card only to pay for purchases of goods and services related to business matters and this, in accordance with the authentication procedures provided by the Issuer. The Customer remains responsible for the Payment Transactions carried out by the Cardholder and the use he/she makes of the Card.

As soon as the Cardholder becomes aware of the loss, theft or a misappropriated and fraudulent use of the Card or the personalized Security Data linked thereto, the Cardholder must inform the Issuer as soon as possible. This request may be performed by the Cardholder or any Authorized User of the Account to which the Card is related.

The Issuer takes into account the opposition request as soon as it receives it from an authorized User. The data corresponding to this opposition is kept for eighteen (18) months by the Issuer in order to meet its legal and regulatory obligations.

The Cardholder is prohibited from making a false declaration to the Issuer under penalty of sanctions provided by law and blocking of the Card by the Issuer.

After expiration of the Card, the Cardholder undertakes to destroy it as soon as possible.

9. Contestations of Payment Operations

The Cardholder and the Customer may dispute unauthorized or improperly executed Card Payment Transactions as described below. Disputes relating directly to a good or service are not receivable by the Issuer, which is only responsible for the Payment Transaction.

9.1. Unauthorized Payment Operations

The institutions will be exempt from liability with respect to Payment orders, even being against the will of the payer, have been obtained as a result of an order received by the institution for whose authentication the established security requirements have been met.

The use of the PIN by a person other than the HOLDER presupposes gross negligence or, fraud on the part of the HOLDER.

The institutions without prejudice to adopting the measures it deems pertinent, is exempt from liability in case of lack of attention to your card by any of the businesses, banks and savings

banks committed to the sale of goods or provision of services, or for incidents of a technical or operational nature in ATMs.

The institutions will also be exempt from liability regardless of the incidents and responsibilities that may arise from the operation carried out between the establishment and the CARD HOLDER.

The institutions exclude, from the scope of its application, Visa's Zero Liability Policy (Visa Global Zero Liability Policy), submitting to current European regulations on the matter.

The system of liability of the ordering party in the event of unauthorised payment transactions, which, in each case, regulates the applicable legislation on the matter, shall apply. Specifically, the HOLDER who does not hold the status of consumer or micro-enterprise in the terms established in Royal Decree-Law 19/2018, of November 23, on payment services and other urgent measures in financial matters, will be obliged to bear the losses derived from unauthorised payment operations resulting from the use of the lost, stolen or improperly appropriated payment instrument by a third party, as long as the loss, theft or misappropriation of the payment instrument is not reported to the institutions.

10. Validity period of the Card

The period of validity of the Card is limited in time. The expiration date is written on the Card. On the expiration date of the Card, and provided that neither Party requests the termination of the Contract or the deactivation of the Card, the Card is automatically renewed. The Issuer will send the new Card to the Customer's business address.

In the event of termination of this Framework Contract or deactivation of the Card, the Cardholder undertakes to give the Card to the Customer, who will return it to the Issuer or destroy it as soon as possible.

11. Deactivation of the Card payment service

The Customer may request the deactivation of the Card at any time. The deactivation will take place within five (5) Business Days from the receipt of the notification by the Issuer.

12. **Guarantee**

In the event of the Card being defective, it can be returned to the Issuer by registered mail with acknowledgment of receipt to be exchanged. If it turns out that the original Card is not defective, fees may be charged to the Customer's Account.

Appendix 1 - Documents required to open a Payment Account per countries

For Spain-based companies:

1. Articles of incorporation in authorized copy (Tittle deeds);
2. Company ID (CIF or NIF) photocopy (NIF if personal company (freelancer);
3. Deed of Power of Attorney (in case the current attorney-in-fact does not appear in the Articles of Incorporation) in authorized copy;
4. Certificate of beneficial ownership in authorized copy;
5. Identity document of the ultimate owners. (in color);
6. Other notarial documents (for example: deeds of change of corporate purpose, change of registered office, change of administrators ...) in authorized copy.

For Sweden-based companies:

1. Certificate of Registration;
2. Certificate of Good Standing;
3. Memorandum & Articles of Association;
4. Recent excerpt from the UBO registry issued within last 3 months or another period (up to you).

For Denmark-based companies:

1. Certificate of Incorporation – Registreringscertifikat;
2. Memorandum & Articles of Association;
3. Recent excerpt from the State registry (issued within last 3 months).

For Estonia-based companies:

1. Recent excerpt from the State registry (issued within last 3 months);
2. Estonia company Ultimate Beneficiary Owners list;
3. Memorandum & Articles of Association.

For UK-based companies:

1. Memorandum & Articles of Association;
2. Certificate of incorporation;
3. Recent Confirmation statement or shareholder registry issued within the last 3 months.

Natural person

-Valid identity document

-If the contract is signed by a person other than the corporate officer: The attorney's proof of authority and identity card

-For each person with the Customer's authority to use the Payment Services: identity card and the attorney's proof of authority

-Any other document required by the Institution for the onboarding process

Legal person (already registered)

-Valid identity document of the corporate officer

-If the contract is signed by a person other than the corporate officer: The attorney's proof of authority and identity card

-For each person with the Customer's authority to use the Payment Services: identity card and the attorney's proof of authority

-Any other document required by the Institution for the onboarding process

Appendix 2 - Rights granted to each User of the TiC Business Account

The different Users profiles are: Owner/Representative (Admin), Employee and Accountant. The rights associated with each User are detailed in Appendix 2.

1. Owner/Representative (Admin)
2. Employee
3. Accountant