Qonto

Terms and Conditions

Payment services framework agreement

Version update: 31 December 2024

The contract is concluded between:

OLINDA, a simplified joint-stock company with a share capital of €298,160.71, listed in the trade and companies register (RCS) of Paris under number 819 489 626 and whose registered office is located at 18 rue de Navarin 75009 PARIS (France), approved by the Prudential Control and Resolution Authority ("ACPR"), located at 4, place de Budapest - CS 92459, 75436 PARIS CEDEX 09 as Payment Institution under number 16958.

Hereinafter referred to as "**the Institution**" 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.

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

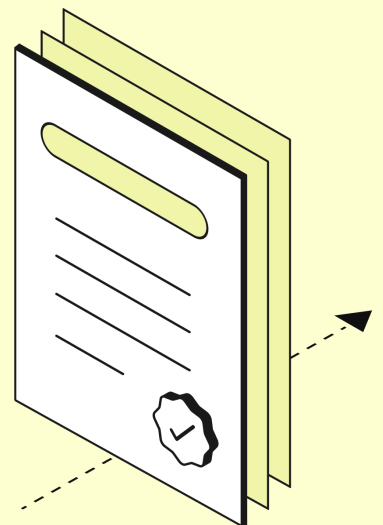Together referred to as the "**Parties**":

Avertissement

The prospect is invited to carefully read this Contract sent online by the Institution before accepting it. The subscription to the Qonto offer is made entirely online by the prospect 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.

Table of content

Title 1 - Your Contract

1.   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 4 of Title 1.

Services provided by the Institution include:

- Holding one or more Payment Accounts
- Issuing Cards
- Execution of the following Payment Transactions associated with the Payment account(s) by:
  - Cards
  - Transfers
  - Direct debits
- Foreign exchange services
- Online capital deposit and cashing of cheques on the Payment Account. It is specified that cheque cashing is provided exclusively to Customers registered in France and online capital deposit to Customers registered in France, Germany or Italy

Certain Services provided by the Institution are subject to their own specific conditions, signed or accepted by the eligible Customer via the Application. The Institution reserves the right to refuse subscription to these services without having to justify the reasons.

(i) **Why are some services not accessible?**

Some services may pose a risk to Qonto which must analyze your eligibility before granting you access.

For example, the following services are subject to their own specific conditions:

- An account aggregation service
- A card payment acceptance service
- A SEPA CORE direct debit issuance service
- A credit facility associated with the execution of Payment Transactions

In case of conflict between the Contract and any specific conditions, the specific conditions will prevail over the Contract if they derogate from it. If the specific conditions are silent, the Contract will apply. If a word or

expression is not defined in the specific conditions, it will have the meaning given to it in the Contract.

As the Customer acts strictly within their professional activities, Articles L. 133-2, L. 314-5 and L. 133-24 of the Monetary and Financial Code apply, allowing derogations from certain protective provisions of the Consumer Code.

2.   Use of services offered

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 – User Rights.

The Customer, through its Owner and its Users, expressly undertakes not to use the Account in an improper manner and to act in accordance with the terms of the Contract at any time.

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

3.   Sign-up Conditions

The Customer guarantees to be acting in their professional capacity and to be registered in France.

The Customer expressly warrants that they own one of the legal forms listed at the following address: Accepted legal forms

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

4.   Pricing terms

4.1. Plans

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

The Pricing Terms define several Plans from which the Customer chooses the one most suited to its needs. The Parties agree that they form an integral part of the Agreement, and their modification is subject to Article

7 of Title 1 of the Agreement. Transaction fees are, unless otherwise specified, debited immediately and billed for the current calendar month.

The Pricing Terms are broken down into Subscription Fees applicable to the Plan chosen by the Customer and Transaction Fees. The Subscription Fee is paid periodically, either monthly or annually, depending on the Customer's Plan. If the Customer decides to change Plans during the Billing Period for a more expensive Annual Plan, only the difference will be charged. If they decide to change Plans during the Billing Period for a less expensive Annual Plan or Monthly Plan, the difference will not be refunded.

The Plan determines the billing frequency of the Subscription Fees, which may be either monthly or annually. An annual Plan commits the Customer for the duration of the Billing Period and the Customer acknowledges that no refund of the Subscription Fee will be made in the event of termination before the end of the current Billing Period.

Customer may change Plans at any time under a Monthly Plan. The pricing terms of that Plan will then apply to the monthly Billing Period following the date of the Plan change.

4.2. Add-ons

Add-ons are additional paid features that can be added to the chosen Plan at the Customer's request. No Add-on is included in the Plan.

The details of features included in each Add-on are specified in the Pricing Terms. As indicated in the Pricing Terms, each Add-on is charged a separate Subscription Fee from that of the Plan with either monthly or annual billing frequency, according to the Customer's choice. However, if the Customer opts for a Plan with monthly billing, they cannot choose an Add-on with annual billing.

4.3. Charging of fees

The fees are billed to the Customer by debiting their Principal Payment Account and, in the absence of sufficient funds, on one of the Additional Payment Accounts if applicable.

If there are no funds for the total amount due in the Principal Payment Account or in 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.

If there are no funds in the Principal Payment Account or in one of the Additional Payment Accounts when payment is due, the charges will be debited once the funds have been replenished as a matter of priority before any Payment Order is executed on the Customer's Accounts.

The Billing Period is one month for a Monthly Plan or one year for an Annual Plan. The Billing Period begins on the date the Customer signs up for the Contract or the date the Customer selects an Annual Plan.

5.   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 unauthorised or fraudulent use of the Personal Area, or any data related to the Personal Area.

If blocked, the Institution shall inform the Customer by any means and shall communicate 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 their Personal Area by contacting the Institution by email or by telephone, at the contact information indicated in Article 15.

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

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

6.   Term

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

This Contract is concluded under the following conditions :

- The validation of the money laundering and financing of terrorism process of identification (for which purposes the Institution may download from public databases, the certificate of incorporation or other available documents on the Customer); and
- Where applicable, for companies in the process of being created, the release of the funds from the capital deposit to the Customer's Account.

Before the conditions are met, certain Services are not available in application of the applicable regulations, with the Contract applying to all other services. This is notably the case for all payment services under Article L314-1 of the Monetary and Financial Code which are not available before the conditions are met.

If these conditions are not met within a period of six (6) 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 decision to terminate.

7.   Amendments

In accordance with Article L. 314-13 (IV), any amendment to this Contract which is significant and adverse to the interests of the Customer will be communicated to the Customer sixty (60) days prior to the date of its proposed application ("the Implementation Date"). The absence of dispute during this period will be considered as acceptance of the amendment brought to the Contract. If the Customer refuses the proposed changes, they must notify the termination of the Contract before the expiry of the aforementioned period. The termination will take effect at the Implementation Date of the amendment to the Contract.

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

Any new services related to the payment account offered by the Institution will be subject to an amendment of the Contract, but for the avoidance of doubt, this shall not include new products, features or services that are ancillary to the Payment Account, such as invoicing or accounting tools.

In the event of a change in the Pricing terms, the amended Transaction Fee will apply as of the Effective Date. Changes to the Subscription Fee will apply as of the first Billing Period following the Implementation Date.

8.   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, within the meaning of "control" provided by Article L. 233-3 of the Commercial Code, upon prior written notification sent to the Customer. 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.

9.   Termination

9.1. Rightful termination

9.1.1. 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 Owner of the account by email to the address support@qonto.com 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 request ("Effective Date").

The termination may also be made directly from the Application or the Site, the Institution reserving the right to refuse or restrict this method of termination at its discretion. In that case, the Effective Date will be at the end of the current calendar month if the balance of the Payment Account(s) is brought down to zero (0) euro by the Customer. If this condition is not met, the request for termination shall not be considered as being received and the fees specified in Article 4 "Pricing terms" shall continue to apply.

If the Effective Date precedes the monthly payment date of the Contract, the Customer will be entitled to the reimbursement of the subscription fee pro rata from the period between the "Effective Date" and the actual monthly payment 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.

9.1.2. Termination by the Institution

As an exception to Article L. 314-13 (V) of the Monetary and Financial code, the Institution may also automatically terminate the Contract by email, with a notice period of thirty (30) days. 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 Customer or a third party of misusing or fraudulently using the Payment Account, or of engaging in any illegal activity, in which case the Institution shall be entitled to terminate the Contract immediately.

9.2. 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 3, threatening the staff of the Institution, communicating false information or refusing communication, upholding a Payment account with a negative balance that the Customer abstain to promptly recharge, suspicion of fraud.

A breach of any specific condition may also constitute a serious breach, in particular, any failure to meet a repayment obligation under the Credit Offer.

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 existing regulations.

9.3. Collective proceedings

In case of collective proceedings of a Party, the Contract may be terminated by email 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. Collective procedure is used to mean: the appointment of an ad hoc agent, a judicial administrator, the opening of

reorganisation or liquidation or insolvency proceedings, or the loss of the licence of the Institution.

9.4. Death of the Customer who is a physical person

In the event of the death of a Customer who is a physical person, confirmed by an official document, the Institution will block the Payment Account(s), then close the Payment Account(s), subject to the settlement of the current Payment Transactions initiated prior to the death and the payment of fees incurred 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).

9.5. Effects of termination of the Contract

The Payment Account(s) shall be closed on the Effective Date, provided that Customer has paid all amounts due under this Agreement. Termination of the Agreement shall not affect any services previously performed or in progress on the Effective Date. Payment Transactions initiated prior to the Effective Date shall not be affected by termination and shall be performed as provided in the Agreement.

In the event of termination of the Contract at the Customer's initiative under an Annual Plan, no part of the Subscription Fee will be refunded to the Customer if the termination date occurs before the end of the Billing Period, in derogation of Article L.314-13 of the Monetary and Financial Code.

If the Customer is registered in Italy or in Spain as a micro-entrepreneur, they can be entitled to the refund of the Subscription Fees pro rata in the event of termination before the end of the Billing Period. Any request for termination will need to be sent to the address support@qonto.com together with the supporting documents indicating their micro-entrepreneur status and the reasons for the refund.

If the termination is initiated by the Institution for serious breach by the Customer, the Institution will not proceed to any refund.

The Institution reserves the right to maintain the Payment Account(s) for a period of fifteen (15) months in order to cover any subsequent disputes

and claims by Payers or to enable the liquidation of any ongoing transactions.

During this period, the expenses detailed in Article 4 "Pricing terms ", 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 termination of the Contract, the Customer must send the Institution the bank details (IBAN) of the SEPA zone bank or payment account in the Customer's name (except

for Customer liquidation or radiation) required for the transfer of the balance held on the Payment account(s). If the request for termination is made by the Customer from the Application or the Website, the Customer is responsible for bringing the balance of the Payment Account(s) back to zero (0) euro, as the termination will not be considered as being received before this condition is met.

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 Article 4 "Pricing conditions", including the subscription costs. These costs are applicable to the Payment Account(s) and are related to the continuing operation of the Payment Account(s).

10.   Liability and Force majeure

10.1. 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 but not limited to financial loss, loss of income, loss of customers, damage to the image, moral damage) 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 (but not limited to asset freezing

measures, blocking of a Payment Transaction for reasons of fight against money laundering and terrorist financing).

10.2. Force majeure

The Parties will not be held responsible for any delay or non-performance that is related to a case of force majeure. Article 1218 of the Civil Code and applicable French case law provides that "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 date of the receipt of such a letter.

If the case of force majeure is final, this Contract is resolved and the Parties are released from their obligations in accordance with Article 1351 of the Civil Code.

11.   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:

- Interruption of the Application for technical maintenance operations or updating published information.
- 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.
- Unavailability, overload or any other cause preventing normal operation of the mobile network used to access the Application.
- Contamination by possible computer viruses circulating on the network.
- 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).
- Abnormal use or unlawful exploitation of the Application.
- Loss by the Customer of their username and/or password or in case of usurpation of their identity.

12.   Personal Data

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

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

13.   Evidence agreement

The Institution is bound by professional secrecy in accordance with Article L.522-19 of the Monetary and Financial Code. 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 for access to all Payment Services.

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

14.   Evidence agreement

As part 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 recognise 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 evidence 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.

The Customer agrees that they will be presumed to have knowledge of any notification on their Personal Area, except where the law explicitly requires a different method of notification.

15.   Communication and Customer Service

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

- By email at support@qonto.com
- By phone: +33 1 76 41 03 08
- By post: OLINDA SAS, 18 rue de Navarin, 75009 PARIS
- Via the Website Help Centre

To send a complaint, the procedure is specified in Article 17 "Claims processing" of this Contract.

The Institution provides on its Website Help Centre a page for most Frequently Asked Questions (FAQs) to assist the Customer with any queries they may have. However, in the event of any conflict between what is written in the FAQ and what is written in this Contract, this Contract shall prevail and shall always be the legally binding document.

16.   Language

The language applicable to contractual relations is French.

17.   Claims processing

The Customer is invited to contact the Claims Service (reclamations@qonto.com) 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) Business Days following receipt of the complaint by the Institution. However, for reasons beyond its control, the Institution may be unable to respond within this period of fifteen (15) Business Days. 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 claim.

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

18.   Non-transferability

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.

19.   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.

20.   Applicable law and competent courts

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

Title 2 - Your Account and your Payment transactions
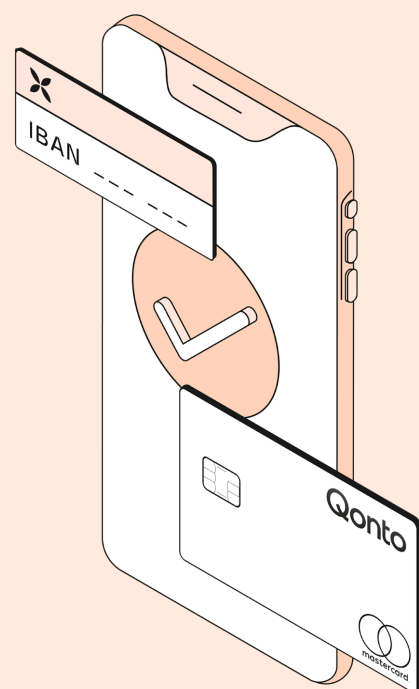
1.   How the Payment Account(s) work(s)

In the event of acceptance of the opening of the Principal Payment Account, the Institution will send a confirmation email to the Customer. The payment account number (IBAN number) opened in the name of the Customer is available in their 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 Economic Area or a third country imposing equivalent obligations in the fight against money laundering and the financing of terrorism.

The Customer may then create Additional Payment Accounts (subject to the Institution approving the Customer's identification documents and within the limit of twenty-five (25) Payment Accounts in total), order Cards and add Users to the Account(s), in accordance with the General Terms of Use of the Card provided for in Title 3.

> **(i) Maximum number of payment accounts**
>
> As a Customer, once you have created the Principal Payment Account, you are free to create Additional Payment Accounts to manage your finances more easily. The total number of Payment Accounts that you can create cannot exceed 25 Accounts (unless we accept to authorize more), but the maximum number varies according to the plan that you have chosen. For more information on the number of payment accounts authorized by the plan, refer to our page on Pricing.

Notwithstanding the foregoing, the Customer may not make any Payment Transactions until the Institution has confirmed activation of all Services. Additionally, the Institution reserves the right, in its sole discretion, to allow the opening of Payment Accounts beyond the twenty-five (25) account limit, and to charge additional amounts for the opening and maintenance of those Additional Payment Accounts.

1.1. Designation of Users

1.1.1. Role of Owner

The opening of an Account is made through the Owner who has the rights to represent and engage the Customer. The Owner 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 authorised 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 can not be engaged.

Since the Owner did not lose the right to represent and engage the Customer, the Payment Account can be set up with the Owner's signature, including in the event a third-party with the ability to represent and engage the Customer challenges the actions of the Owner with the Institution or claims that they should be the Owner. A corporate officer of the Customer could nevertheless ask the Institution for some information about the Account (especially bank statements and the balance of the Payment Account).

In case of a dispute between several persons with rights to represent and engage the Customer, the Institution reserves the right to suspend or close the Payment Account if the funds of the Customer should incur any risks.

1.1.2. Role of Administrators and Employees

Moreover, the Customer may give power of attorney to Administrators or Employees authorised to use the Services on their behalf and for their account, and under their entire responsibility. The power of attorney form is available in the Personal Area of the Payment Account's Owner or Administrator. The power of attorney will only take effect upon receipt by the Institution of the duly completed form and the required supporting documents. The power of attorney ceases automatically upon the death of the Owner or the Administrator who has issued it. The power of attorney may be revoked by the Customer at any time by informing the Institution through their Personal Area without undue delay. If the notification is not made or is made late, the power of attorney remains valid and the Institution can not be held liable.

The Customer expressly discloses the obligation of professional secrecy relating to the Payment Account data in respect of Users.

The Customer determines for each User the scope of the rights they have on the Payment Account(s). Each User is assigned Personalised Security Credentials of their own, in order to access their Personal Area. The Personal Area of each User is personalised according to the rights granted to them by the Customer. The different Users profiles are: Owner,

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

1.2. Personalised Security Credentials

The Customer must take all reasonable steps to maintain the confidentiality and security of their Personalised Security Credentials. They also undertake to make users aware of the preservation of the confidentiality and security of their own Personalised Security Credentials.

The Customer (and each User) needs to stay vigilant before accepting some sensitive transactions and carry out all required checks, at the risk of bearing full responsibility and its consequences by pursuing said transaction.

(i) **Examples of sensitive and suspicious transactions:**

- Fake consultants from the Institution who contact the Customer under the guise of the existence of fraudulent transactions on their Account and ask them to undertake a number of validation such as connecting a new device or changing a password.
- The presentation of fake offers of credit from the Institution at derisory interest rates compared to the market or to other financial products with highly competitive returns.
- The proposal to invest in unusual products or markets offering considerable financial gains and/or presented as non-risky.

These examples point to a high risk of fraud and heavy financial losses for the Customer.

The Customer (and each User) undertakes not to communicate their Personalised Security Credentials 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 said Provider is approved or registered for the aforementioned services, and that they enter their Personalised Security Credentials 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 authorised 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.

1.3. 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/these statement(s) is/are available in their Personal Area.

The Customer undertakes to check the contents of the Transaction Statement(s) 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.

1.4. Balance of the Payment Account(s)

The balance of the main Payment Account and each Additional Payment Account associated with it form a single, indivisible and global balance. The creation of an Additional Payment Account does not imply any special allocation of the sums deposited in it, unless the Institution explicitly consents. For the implementation of this clause, the Customer acknowledges that the Institution may need to move funds between the Principal Payment Account and any Additional Payment Accounts to honor debit operations occurring on any of these accounts. This includes but is not limited to the deduction of Fees by the Institution, seizures or administrative seizures to third-party holders (SATD), unpaid card transactions or direct debits.

As the Customer's Payment Account balance can not 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.

Exceptionally, and without any obligation of payment facility, the Institution may be required to pay one or more Transactions, the amount of which would be greater than the balance of the Customer's Payment

Account (in particular in the case of a Transaction by card without prior authorisation, or issuance of unpaid card or a direct debit).

In this situation, the Customer undertakes to send funds to each Payment Account having an insufficient balance without delay in order to restore a positive or zero balance. In case of non-compliance with these obligations, the Institution reserves the right to suspend or close the concerned Payment Account and/or the other Accounts, and to use all means to recover the amounts due at the Customer's expense.

> (i) **Why can't your account be negative? ?**
>
> As a payment institution, Qonto cannot grant you an overdraft. However, your account may occasionally show a debit balance for strictly technical reasons, for example following a card payment that does not require systematic authorization. In this case, you must fund your account without delay.

1.4.1. Account funding by payment card

When the Account is opened, the Customer may fund the Account by making a payment with a payment card issued by a third-party payment service provider. The charges for this card payment transaction are determined by the contractual agreements between the Account holder and the issuing payment service provider.

The full amount of this transaction is credited to the balance of the main Payment Account. In accordance with the Contract, this balance may subsequently be used to pay any Charges or to bring the negative balance of the Account back to a positive balance.

By making a payment card payment to the Account, the Cardholder accepts that the Establishment may subsequently initiate a card payment transaction in the event of (i) an insufficient balance to enable payment of the Charges, or (ii) to enable the negative Account balance to be returned to a positive balance. Cardholders may withdraw their consent at any time from their Customer Area.

1.5. 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 the 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.

The balance will be deposited with the Caisse des dépôts et consignations (French public sector financial institution) and the sums may be claimed by the Customer or their beneficiaries for twenty (20) years from their deposit. The Institution may debit an inactive account management fee each year, to the extent permitted by law.

1.6. Fight against money laundering and terrorist financing

As a Payment Service Provider, 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, Articles L. 561-2 and following of the Monetary and Financial Code apply throughout the term of this Contract. In particular, 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. The Institution may refuse to execute or may reject any unusual Payment Transaction, debit or credit, of the Payment Account.

In addition, the Customer is informed that the Institution may be required to report to the national Financial Intelligence Unit (TRACFIN) 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.

1.7. Protection of funds

> **(i) How are your funds protected**
>
> Your money is 100% secure because the funds deposited in your Qonto account must be protected completely separately from our own funds, in accordance with the laws and regulations that apply to us.
>
> Regardless of how customer funds are protected by Qonto, it is important to note that all these protection methods cover 100% of our customers' funds and have been subject to prior authorization by the ACPR, as required by the rules applicable to Qonto.

In accordance with Article L. 522-17, I of the French Monetary and Financial Code, the Customer's funds are either:

- deposited at the end of each Business Day in a segregated account opened with one or more credit institutions, or
- invested in units of a fund, fully covered by a guarantee granted by a credit institution, or
- invested in eligible short-term money market funds.

The Customer's funds are protected against any recourse by other creditors of the Institution, including in the event of enforcement proceedings or insolvency proceedings against the latter.

1.8. Blocking of the Account

For regulatory or operational reasons, or reasons relating with the security of Payment Transactions carried out by the Customer, the Institution reserves the right to apply all necessary restrictive measures on the Account and/or the Payment Transactions (such as the suspension or temporary blocking of the Account or of any Payment Transaction). Unless there is a legal impossibility or prohibition, the reason behind the restrictive measure will be given to the Customer.

2. Unavailability of assets

All funds credited to the Customer's Account(s) may be blocked on the action of the Customer's creditors by means of protective attachment or seizure of garnishment on one of the Payment Accounts, served on the Institution by a bailiff or by administrative seizure to a third-party holder. These actions result in the invoicing of expenses by the Institution to the Customer, detailed in Appendix 3 "Special Operations".

2.1. Seizure

As of the service of the seizure, the Institution is required to declare the balance of the Payment Account(s) up to date of the seizure. For a period of fifteen (15) Business Days from the day following the date of the seizure during which the sums are unavailable, the balance of the Payment Account(s) may be affected by the Payment Transactions whose origin is prior to the date of the payment entry. At the end of this period, the Institution will make available to the Customer amounts exceeding the total of the seizure.

In case of seizure of garnishment, the Institution proceeds to the payment on presentation of a certificate issued by the registry of the court attesting that no challenge was formed in the month following the denunciation of the seizure. If the Customer has stated, in writing, not to contest the seizure, payment may be made before the expiry of this period.

In the event of a provisional seizure, the creditor must notify the Institution of its conversion into seizure-attribution. Payments made by the Institution will then be made in accordance with the above provisions.

2.2. Administrative seizure to third-party holder

The French Treasury can lay claim to the sums due to it by way of notice to third-party holders. Upon receipt of the notice to a third-party holder, the

Institution will block the Customer's Account(s) under the same conditions as those described above.

The Institution will pay the funds to the Public Treasury within a period of thirty (30) days except in the event of release from the Public Treasury or recourse initiated by the Customer.

3. Execution of payment transactions: general rules

3.1. Payment Transaction

A Payment Transaction is independent of the underlying civil or commercial obligation between the Customer and the Payment Beneficiary. The Institution therefore remains foreign to any civil or commercial dispute that may arise between the Customer and the Beneficiary. The Institution shall not be liable for duly executed Payment Transactions in the event of an error by the Customer in the Beneficiary's bank account details or identity.

A Payment Transaction may be initiated by the Customer giving a Payment order directly (transfer), by the Customer giving a Payment Order through the Payee (card) or by the Payee (direct debit).

3.2. Security of payment instruments

The Customer will take reasonable steps to maintain the security of their Personalised Customer Security Data. Upon knowledge of loss, theft, misappropriation or any unauthorised 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 15). The Customer can also claim a direct opposition from their Personal Area.

If the blocking request was made by telephone, the Customer must confirm their request in writing (by post 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 their 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. A written confirmation of this opposition will be sent to the concerned Customer by email or in their Personal Area.

In case of blocking (or opposition), the Institution provides the Customer, at their request and for eighteen (18) months from the blocking (or opposition), the elements allowing them to prove that they have successfully blocked (or opposed).

Any misrepresentation by the Customer or Users may result in legal action.

Notwithstanding Article L.133-19, I of the Monetary and Financial Code (in accordance with Article. L. 133-2 of the same code), in case of loss or theft of the Personalised Security Credentials, the unauthorised Payment Transactions made prior to notification of the opposition shall be borne by the Customer. Payment Transactions carried out after the opposition are borne by the Institution, except in the case of fraud by the Customer.

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.

The Institution reserves the right to block the payment instrument in case of (i) risk to the security of the payment instrument, (ii) suspicion of unauthorized or fraudulent use of the payment instrument, or (iii) risk that the Customer may be unable to subsequently fulfill their payment obligation related to a Payment Transaction made with this payment instrument.

3.3. Strong authentication

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

- accesses the Customer's Online Payment Account(s);
- initiates an Electronic Payment Transaction (except in the event of transfer to another account held in the name of the Customer);
- executes a Transaction through a means of remote communication, which may involve a risk of fraud in payment or other fraudulent use.

Strong Authentication is performed by the validation of a notification on the Application (knowledge component) on a phone previously associated with the User, in the dedicated field of the Application

(possession component). The Customer will not be able to deactivate the Strong Authentication.

In case of a Payment Transaction validated by Strong Authentication, the Institution can refuse to refund the Customer with the reason that the latter acted with gross negligence, did not intentionally meet their obligations to preserve the Personalised Security Credentials from their Account or in the event of a Customer committing fraud. Furthermore, if the payment was initiated following a Strong Authentication, the transaction will be considered as having been validated by the Customer, unless the latter provides evidence to the contrary.

4.   Contestation of Payment Transactions

The Parties agree to derogate from the provisions of Article L.133-24 of the Monetary and Financial Code. The dispute periods specific to each Payment Transaction are defined in the following articles.

5.   Issuing Cards

The Institution issues physical and virtual Cards according to the conditions detailed in Title 3. Cards issued that are not included in the Customer's Plan are subject to Card fees.

6.   Execution of Payment Orders by transfer

6.1. 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 euro, or in a currency covered by the Institution, under the conditions described in section 6.3 below. The list of currencies covered is indicated in the Personal Area of the authorised User.

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

- The Payment Account where the Customer intends to initiate the Payment Transaction;
- 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 their bank details (IBAN);
- The execution date (in the absence of indication of date, the Transfer Order occurs immediately);
- The reason for payment;
- The currency.

The User is invited to check all of this information before validating their 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 their 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 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.

6.2. Transfers denominated in euro

The Transfer Order must comply with SEPA rules set forth in the "SEPA Credit Transfer Rulebook." The User has the option of issuing Transfer Orders that are instant or standard, one-time or recurring.

For instant Transfer Orders, the Transfer Order is deemed received by the Institution once the User has definitively given their consent to the Order, according to the procedure indicated in the Personal Area ("Date of receipt"). It is expressly agreed that the Orders for Instant Transfers will be executed by the Institution not later than the end of the Working Day following the Date of Receipt of the Order by the Institution. If the Date of

Receipt is not a Working Day, the Payment Order is determined to be received on the next Working Day. The Parties also agree that any Payment Order validated on a Working Day after 14:00 shall be received on the next Working Day.

With respect to 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 Working Day, the Institution will execute the Transfer Order on the next Working Day.

6.3. Foreign currency-denominated Transfers

The Customer has the option to issue a Transfer Order in a foreign currency. For this purpose, the authorised User enters the details of the Transaction, specifying the amount in the foreign currency. The Institution will provide the User with a quote for this transaction, including applicable fees. If the User accepts the quote, they follow the procedure indicated in their Personal Area in order to give their final consent to the Transfer Order in foreign currency.

The execution time of Transfer Orders in foreign currency is dependent on the foreign currency chosen as well as the third-party partners with whom the Institution works to carry out said Transfer Order.

The Institution of the Beneficiary and the service provider of the Institution enabling to carry out the Transfer Orders in foreign currencies may reject the transfer due to information that is missing, incomplete, incorrect or closed account. In some cases, foreign exchange fees and/or additional fees may be applied and deducted directly from the transaction amount. The funds are paid into the Payment Account of the Customer according to the exchange rate on the date of the return of the funds. There can be a delay between the date of rejection by the Institution of the Beneficiary and the payment of funds to the Customer.

The Institution is not responsible for these fees and these timeframes.

6.4. 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, unauthorised 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 Terms (Article 4 of Title 1) if the refusal is objectively motivated.

6.5. Contestations concerning Payment Orders by Transfer

If the Customer wishes to contest a Payment Order by Transfer that they have not authorised or that has been incorrectly executed, they must contact the Institution's Customer Service by phone 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.

Unless the Institution has reasonable grounds to suspect fraud by the Customer or gross negligence on the part of the Customer within the meaning of Article L. 133-19, IV of the Monetary and Financial code, the Institution shall reimburse the Customer for the amount of the Payment Transaction immediately after receiving the contestation, and in any event not later than the end of the following Working Day. The Institution restores the Account to the state in which it would have been if the Unauthorised Payment Transaction had not taken place. The Institution reimburses the Customer under the same conditions when the Payment Transaction was initiated by a payment initiation service provider.

Fees listed in Article 4 of Title 1, Pricing terms, may be levied in the event of an unjustified contestation of a Payment Transaction. The Institution can not 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.

If the Institution is unable to recover funds, the Customer may request the Institution to provide any relevant information it has in order to document its legal recourse to recover the funds.

In case of duplication, error or fraud, the Customer can ask the Institution to request a return of the funds to the payment service provider of the

beneficiary for a contested Payment Transaction by transfer. To do so, the Customer needs to contact the Institution within a maximum of ten (10) days after the issuance of the contested Payment Transaction by transfer. The Institution reserves the right to accept the request for a return of funds and will not guarantee the effective return of the funds.

6.6. Receiving Transfers

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

Notwithstanding Article L.133-8, IV of the Monetary and Financial Code, the Institution may revoke an incoming transfer and return the funds to the issuer's account without the Customer's consent, in particular if the Institution has reasonable grounds for suspecting fraudulent use of the account by the Customer.

The Institution credits one of the Customer's Payment Accounts not later than the end of the Working Day 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).

7. Direct debits

7.1. SEPA core and B2B direct debits

The Customer has the option of paying by SEPA direct debit for persons with whom they have a business relationship (the "Creditors").

For the purpose of this article, the term "Maturity Date" means the date of interbank settlement, i.e. the date of debiting the Customer's Account.

7.2. Direct Debit Mandate ("Mandate")

The Customer who accepts the SEPA Direct Debit as a method of payment must complete the Direct Debit Mandate delivered by their Creditor and return it to them accompanied by a bank statement, with the BIC and IBAN of the Payment Account selected to be debited. The physical person signing the Mandate must be a person authorised by the Customer for

this transaction. The Customer undertakes to inform the Institution of the signature of any Direct Debit Mandate.

By signing the Mandate, the Customer expressly waives the right to reimbursement of authorised and correctly executed transactions.

The Customer undertakes to inform the Institution immediately of any change to the Direct Debit Mandate. The Institution can not be held responsible for an incorrectly executed operation due to a lack of information from the Customer.

The Customer may also revoke the Direct Debit Mandate at any time within their Personal Area or by contacting the Institution. For this purpose, they shall communicate the unique Reference of the Mandate to the Institution. The revocation must be requested by the Customer at the latest before the end of the Working Day preceding the Expiration Date of the next withdrawal operation provided for by the Mandate.

The revocation entails the definitive withdrawal of the Customer's consent to the execution of the Mandate. The Institution will refuse all the Direct Debit Orders presented after the revocation of the Mandate by the Customer.

A Direct Debit Mandate for which no SEPA Direct Debit Order has been submitted for a period of thirty-six (36) months becomes null and void. In this case, the Customer must enter and validate a new mandate.

7.3. Direct Debit Orders

The Customer is informed that their Creditor is required to provide them with advance notice of at least fourteen (14) calendar days before the SEPA Direct Debit Due Date, unless there is a specific agreement between the Customer and the Creditor in the Direct Debit Mandate.

Upon receipt of this notification, the Customer has the opportunity to verify compliance with their relationship with the Creditor. The Customer must ensure that they have sufficient funds in their Account on the Due Date.

In the event of disagreement, the Customer is invited to immediately address their Creditor so that the latter suspends the transmission of the Direct debit order or issue an instruction for the revocation of the original Direct Debit Order.

The Institution receives the Direct Debit Orders transmitted by the Creditor's payment service provider no later than the day before the Due Date. For a first recurring charge or for a one-off charge, the Institution will verify the existence of the Customer's consent and the validity of the Mandate. In case of inconsistency or incomplete data, the Institution may reject the relevant direct debit Transaction.

For the following recurring direct debits, the Institution verifies the consistency of the mandate data with the data already recorded and the data of the Transactions. In case of inconsistency, the Institution will contact the Customer.

The Institution debits the Customer's Payment Account of the amount of the Transaction when no event is against it and provided that the Payment Account has a sufficient provision. The Customer will receive a notification in their Personal Area to inform them of the amount debited from their Account.

7.4. Interbank rejections

The Customer is informed that prior to the due date, the Institution may have to make interbank rejections towards the Creditor's payment service provider (for example if the Customer's contact details are incorrect).

In addition, as of the due date and within two (2) Working Days, the Institution may make interbank returns to the Creditor's payment service provider for bank reasons (e.g. insufficient provision on the Customer's Payment Account).

The Customer will be informed of these events by notification in their Personal Area.

Prior to the Due Date, the Customer may request the Institution to refuse a deduction, regardless of the reason.

7.5. Direct Debit Order dispute

The Customer has no right to reimbursement of the Direct Debit Transactions that they have authorised. It is specified that the Customer has no right to reimbursement if the mandate does not indicate the exact amount of the debit transaction and the amount of the transaction exceeds the amount to which the Customer could reasonably expect.

The Customer may request the refund of an unauthorised deduction within thirteen (13) months from the date of debiting their account, under

penalty of foreclosure. This period shall be reduced to seventy (70) days if the Beneficiary's payment service provider is located in a State that is not a member of the European Union or the European Economic Area.

8.   Cheque cashing

The Customer registered in France has the option of sending cheques to the Institution to be credited to the Payment Account of their choice.

An authorised User must complete the cheque deposit form on their Personal Area by selecting the beneficiary Payment Account and indicating in particular the cheque number, the payer and the date of issue.

The Customer must send the cheques to the address indicated in the Application or their Personal Area.

The Customer is required to keep a copy of the cheques delivered to the collection. This copy may be requested by the Institution in case of loss of the original.

Cheques will be credited to the Payment Account within between fifteen (15) and sixty (60) Working Days following receipt by the Institution, subject to the following conditions:

- The cheque must be made payable to the Customer and refer only to its company or corporate name,
- The cheque is issued by a French credit institution and denominated in euro,
- The amounts in figures and in letters agree,
- Presence of the signature and the date of issue of the cheque,
- Absence of overload, scraping or any other indication that may suggest falsification (unusual colour, abnormal thickness).

The Institution reserves the right to refuse a cheque deposit. In case of refusal to cash a cheque, the Customer will be informed by notification in their Personal Area.

In the case of a dispute or an outstanding debt due to a bounced cheque, the Customer expressly agrees that the Institution will reverse the amount of the cheque debited from the concerned Payment Account.

9.   Financial Tools services

The Institution offers a range of Financial Tools designed to assist the Customer in managing their business, including accounting setup, cash flow management, employee expense management, supplier and customer management, and payment of charges.

9.1. General provisions

The Financial Tools Services provided by the Institution are ancillary to the Payment Account and accessible through the Application. Since Financial Tools Services do not constitute payment services within the meaning of Article L. 314-1 of the Monetary and Financial Code, certain provisions of the Contract specific to payment services do not apply to this Article 9. In particular, by derogation from Article 7 of Title 1 - Modification, if a proposed modification of this Contract regarding the Customer only modifies the provisions applicable to Financial Tools Services, it will be communicated to the Customer thirty (30) days before its proposed application date, with the rest of the article remaining unchanged.

The Customer is informed that access to some of these Financial Tools Services may depend on the Plan chosen by the Customer.

These services never constitute accounting, social, legal or tax advice. The Institution cannot be held responsible for decisions and choices made by the Customer based on information provided by the Financial Tools Services.

The Institution does not guarantee that these services are adapted to the Customer's particular situation. The Customer must verify before using these services that they are adapted to their particular situation.

9.2. Specific provisions of the invoicing service

9.2.1. Editing and sending invoices

The Institution provides the Customer with an invoice management and editing tool in the Personal Area allowing them to generate invoices and send them to their own customers. The tool allows the Customer to create and send customized quotes and invoices by email using pre-registered data, convert validated quotes into invoices, track payments, manage automatic invoice numbering and manage invoice cancellations through credit notes.

Invoice editing: The templates from the invoice editing tool must be customized to adapt to the Customer's activity, who must verify before

using it that it is suitable for their particular situation. The Institution does not guarantee that the tool is suitable for all use cases or the Customer's particular situation.

Sending and format of invoices: Invoices are sent to the Customer's customers at the address indicated by the Customer. It is the Customer's responsibility to ensure that their customer accepts this invoicing method. Invoices issued in France are in structured format within the meaning of Article 289 VII, 3° of the General Tax Code. All invoices issued from the Institution by French customers will be transmitted to the Institution's Partner Dematerialization Platform, which will process them in accordance with the conditions provided by Article 289 bis of the General Tax Code, Annex II, and transmit them to their recipients' partner dematerialization platform, if they have one.

9.2.2. Receiving and importing invoices

When receiving invoices from their own suppliers, the Customer can transfer and automatically import these invoices into the Application and prepare payment through automatic extraction of invoice data (beneficiary, IBAN, amount, etc.). The Customer is informed that Article 9.5 of this Title applies to this functionality.

9.2.3. Receiving e-invoices

The invoicing service offered by the Institution is an electronic invoicing service. This service allows the Customer's suppliers to send electronic invoices through the Institution's Partner Dematerialization Platform service.

Designation of the Institution as Partner Dematerialization Platform: The Customer agrees to (i) designate the Institution as Partner Dematerialization Platform, (ii) have the Institution register them in the central directory provided for by Article 289 bis of the General Tax Code, (iii) designate the Institution as PEPPOL Service Provider to register them as a PEPPOL participant, allowing their suppliers to transmit electronic invoices from their own Partner Dematerialization Platform.

The Customer agrees to receive through the Application electronic invoices issued by their suppliers and received through the Institution's Partner Dematerialization Platform service. Suppliers will be able to see that the Institution is the Customer's Partner Dematerialization Platform. The Customer using the electronic invoice reception service agrees to waive the Institution's professional secrecy obligation towards (i) other Partner Dematerialization Platforms, (ii) public authorities managing the aforementioned directory and (iii) their suppliers' PEPPOL Service Providers. The Institution must share Customer information as required by

Article 242 nonies H, II of the General Tax Code, Annex II, in order to create the Customer's electronic invoicing address allowing them to receive electronic invoices from their suppliers.

The Customer may choose to designate another Partner Dematerialization Platform or not use the service and revoke the designation mentioned above. To do this, the Customer can modify their settings from the Application, follow the dedicated FAQ or contact the support.

> (i) **Why are our invoicing services evolving ?**
>
> To help you smoothly prepare for the electronic invoicing reform, Qonto is evolving its services by becoming your Partner Dematerialization Platform, a status obtained from the General Directorate of Public Finance.
>
> You want to use another Partner Dematerialization Platform? No problem, you can modify this from the Application by following the FAQ.

9.3. Dashboard, data export and third-party tool synchronization

The Institution provides the Customer with a dashboard in the Personal Area showing the Customer's financial situation, cash flows, and categorizing expenses and income.

The Customer can synchronize information, data and documents from the Financial Tools Services with third-party tools. The Institution is not responsible in this case for the Customer's use of third-party tools. It does not guarantee the proper functioning, availability of third-party tools, their suitability for the Customer's particular situation or their interoperability with the Institution's services.

The Customer can export information, data and documents from the Financial Tools Services from the Application, for example to enable accounting reconciliations. As the Institution does not offer reversibility services, the Customer is informed that in case of Contract termination, they are responsible for exporting the data and reintegrating it into their replacement tools on their own initiative.

9.4. Document digitization

The Application allows the Customer and its Users to digitize invoices, receipts, expense reports and other supporting documents, including but not limited to, from their mobile phones. Once digitized, these supporting documents are accessible in the Customer's Personal Area. As part of its certified documents service, the Institution applies an electronic signature certificate to documents that the Customer requests to be certified for use as digitized supporting documents (access to this service depends on the Customer's Plan). The Customer is responsible for keeping the original supporting documents by their own means, in compliance with current regulations, particularly for potential tax authority audits.

The Customer can use automatic data extraction features for these supporting documents (such as supplier name, VAT number, amount, etc.). The Customer is informed that Article 9.5 applies to this feature.

9.5. Use of automatic data extraction features

The Institution allows the Customer to perform automatic data extraction from documents imported by Users as part of the Financial Tools Services. This feature enables the detection of key data from these documents (counterparty name, transaction amount and type, IBAN, etc.), particularly through optical character recognition technologies.

The Customer is informed of the technical limitations inherent to this technology. They must therefore ensure the completeness and accuracy of the extracted data before validating any operation or making any management decision based on this data. The Customer is presumed to have performed this verification if they validate a payment operation from the Application based on the extraction result.

Title 3 - Your Cards
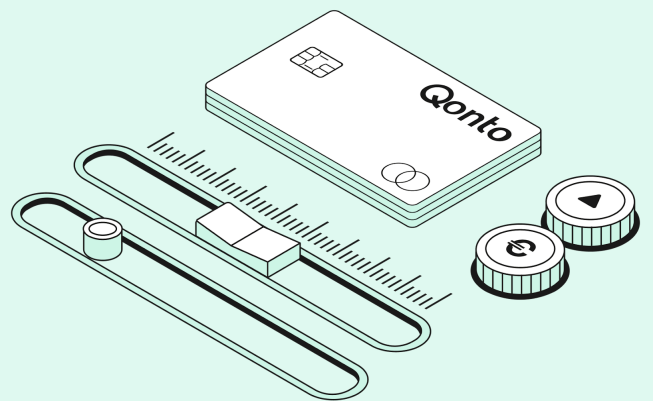
This section relates to the Professional Card and defines the conditions of subscription, operation, and use of the Card by the Cardholder. The conditions of this section remain applicable under the same conditions except modifications made by the Issuer notified to the Cardholder and to the Customer within a notice period of thirty (30) days.

The Card is a payment card with systematic authorisations 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 and remote Card Payment Transactions (RCPT).

1. Obligations of the Cardholder and of the Customer

After having read and accepted these general terms of use of the Card, the Owner undertakes, under their 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.

The Customer is responsible for the Payment Transactions made by Card by the Cardholders.

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 they have designated.

Cards issued by the Institution are physical or virtual Mastercard payment cards with systematic authorisation. The Cards are attached to a Customer's Payment Account and are issued in exchange for the payment of fees detailed in Article 4 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, they will be invited to create their Personal Area, with their own Identification Data. The Cardholder must transmit the information and documents requested by

the Institution through their 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 spending caps, within the limits 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 security and confidentiality reasons, the Cardholder determines his or her secret code in his or her Personal Space.

Before receiving the Card, the Cardholder can make purchases online or in a store via a Wallet Service, thanks to the digital reproduction of the Card.

The Institution reserves the right to set a spending limit on this digitally reproduced Card, as long as the physical version has not been used at least once.

Upon receipt of the Card, the Cardholder is invited to activate it in accordance with the instructions provided by the Issuer in the mailing.

The Cardholder must sign the Card in the space provided for this purpose. The Cardholder is prohibited from making any other physical or functional alteration to the Card.

3.2. Virtual card

The virtual card is accessible directly from the Personal Area of the Cardholder. For security reasons, a 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 authorisation. Therefore, prior to any effective execution of a Payment transaction, the Payment Account balance is verified by a request for authorisation. If the authorisation 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 Orders made by the Cardholder.

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

4.2. Payment Transaction Orders in foreign currencies depending on the Network Rules

The Card issued by the Issuer operates as an international payment card, allowing currency exchanges by the Network. Card Payment Orders may be given in any currency defined by the Network, according to the specific conditions of the Network. The exchange rate that may be applicable is that in effect on the date of the processing of the Transaction by the Network.

4.3. Personalised Security Credentials

The Card is a payment instrument with Personalised Security Credentials. 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 they receive the instruction.

4.4. Using Personalised Security Credentials 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 its 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 unauthorised third-party. The Cardholder is reminded that merchants, e-commerce sites, the Customer, the Issuer, representatives and any other partners are not authorised 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, they can reset it from their Personal Area.

Prior to any professional journey abroad, the Cardholder is advised to contact the Issuer for applicable security measures.

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 Network. 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 Personalised Security Credentials in remote payments

The Cardholder may make Remote Card Payment Orders. For this purpose, they will be asked to provide the following Personalised Security Credentials: the Card number, the validity date and the visual cryptogram on the back of the Card. For each new Payment transaction, and depending on the case, the Cardholder must respect the Strong Authentication procedure and where applicable 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 and, possibly in certain circumstances, other additional charges not within the Institution's control.

4.6. Saving the Card in a Wallet Service

The Cardholder can save their Card on a Wallet Service, provided by a third party to the Institution. This service enables to save the details of a payment card – including a virtual card – in a dedicated mobile application and to therefore be able to carry out Card Payment Transactions using a mobile phone. The Cardholder will have previously approved saving these Card details.

The operating methods of the Wallet Service are governed by the general terms of use of the Wallet Service provider, and have previously been agreed by the Cardholder. Only the Google Pay and Apple Pay Wallet Services are compatible with the Cards issued by the Institution.

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 payment: Consent is provided by the communication of Personalised Security Credentials 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.

Payment using a Card saved in a Wallet Service: the consent terms for the Card Payment Transaction are governed by the general terms of use of the Wallet Service provider, previously accepted by the Cardholder. The consent to a Payment Transaction by Card saved in a Waller Service made from a mobile telephone, and whose saving has previously been accepted by the Cardholder, is irreversible.

Any Card payment transaction authorised by the Cardholder in one of the forms described above is irrevocable.

6.   Receiving and executing the Card Payment Order

The Parties agree that a Card Payment Order is deemed to be received by the Issuer at the time this transaction 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.   The Cardholder's Personal Area

The Cardholder has a Personal Area accessible via the mobile application or the website using the identification data. In their Personal Area, the Cardholder has access to the following features: view of information related to their Payment Card, details of transactions made with the Card, declaration of loss or theft of 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 they make 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 Personalised Security Credentials linked thereto, the Cardholder must inform the Issuer as soon as possible in order to block the card. This request may be performed by the Cardholder or any authorised User of the Account to which the Card is related, directly from their Personal Area.

The Issuer takes into account the card block request as soon as it receives it from an authorised User. The data corresponding to this card

block 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 Transactions

The Cardholder and the Customer may dispute unauthorised 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. Unauthorised payment transactions

The Customer who wishes to contest an allegedly unauthorised Card Payment Transaction must write to the Issuer's Customer service as soon as possible after becoming aware of the transaction and send the contestation file, duly completed, with required attachments, at the latest within eight (8) weeks following the registration in the Account of the Transaction. This period is reduced to seventy (70) days if the Beneficiary's payment service provider is located in a State that is not member of the European Union or within the European Economic Area.

Unless it has good reason to suspect that the Cardholder or the Customer acted fraudulently or with gross negligence, the Issuer shall reimburse the Customer for the amount of the Transaction. The Issuer restores the debited Account to the state in which it would have been had the unauthorised Payment Transaction not taken place.

In the event of loss or theft of the Card or Personalised Security Credentials, the Customer bears the losses of unauthorised Transactions made prior to the notification of the contestation. Transactions made after the contestation are borne by the Issuer, except in the event of fraud or gross negligence on the part of the Customer.

Fees may be levied in the event of an unjustified challenge to a Transaction.

9.2. Incorrectly executed Payment Transaction

Any incorrectly executed Payment Transaction due to the fault of the Issuer must be reported in writing by the Cardholder or Customer to the Customer service within eight (8) weeks from the debit date. This period is reduced to seventy (70) days if the Beneficiary's payment service provider is located in a State that is not member of the European Union or is not in the European Economic Area, whatever the currency used for the Payment Transaction.

The Institution restores the debited Account to the state in which it was if the incorrectly executed Payment Transaction had not occurred. The value date on which the Customer's Payment Account is credited is not later than the date on which it was debited, except where the Institution is unable to do so for reasons outside its control.

10.   Validity period of the Card

The validity period 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.

Appendices
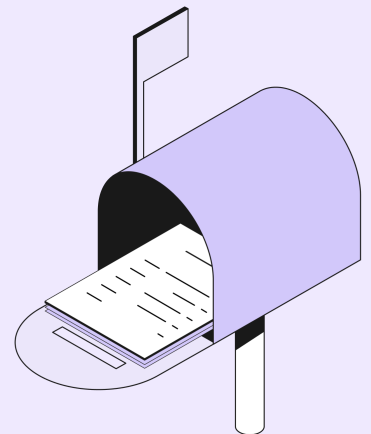
Définitions

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

Account information services provider	Refers to an authorised or registered payment service provider that is distinct from the Institution and who, with the consent of the Customer, can access their Account(s).
Accountant	Refers to a natural person of legal age 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 or the Team and cannot hold a Card.
Add-ons	Refers to additional paid features that can be added to the chosen Plan at the Customer's request. No Add-on Module is included in the Customer's Plan.
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 books, in order to provide Payment Services and manage cash more effectively. This feature is only offered to Customers who have subscribed to a Smart Solo, Premium Solo, Essential Team, Business Team or Enterprise Team package.
Administrator	Designates a natural person of legal age, mandated by the Customer, having all the rights on the Account except for the possibility to open or close the latter.
Annuel Plan	Means a Plan in which access to Services is offered in exchange for an annual subscription fee.
Application	Refers to the Application provided by the Institution to give access to the Personal Area.
Beneficiary	Refers to a legal or natural person, recipient of a Payment Transaction issued by the Customer.

Billing Period	Means the billing period applicable to the payment of Subscription Fees under a Monthly or Annual Plan.
Business Day	Refers to a calendar day corresponding to the operating hours of the Customer service as indicated on the Website or the Application.
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.
Card Fees	Refers to the fees charged by the Institution for issuing Cards not included in the Customer's Plan.
Cardholder	Refers to a natural person mandated by the Customer to use a Card in the strict context of the Customer's professional activity.
Contract	Refers to this document and its appendices, any special conditions and any amendments to this document.
Credit Offer	Refers to the offer through which the Institution undertakes to make available to the Customer, subject to eligibility conditions, a Credit to fund one of more Payment Transaction(s) carried out by the Customer, in compliance with Article L. 522-2, II of the Monetary and Financial Code. The specific terms of the Credit Offer are signed separately.
Customer	Refers to a natural or legal person acting in the course of their professional activity and in whose name one or more Payment Account(s) are opened in the books of the Institution.
Customer Service	Refers to the customer support whose contact details are available in Article 15 of the General Terms.
Date of application	Refers to the date on which a modification of the Contract, notified to the Customer under the conditions of Article L. 314-13 of the Monetary and Financial Code, becomes applicable to the Customer.
Employee	Refers to a natural person of legal age, mandated by the Customer or added by the Manager, who has restricted rights to the Account. They can make purchases by Card.

Financial Tools	Refers to the range of support services in managing their business, particularly in establishing their accounting, cash flow management, employee expense management, supplier and customer management, and payment of charges.
Identification data	Refers to the combination of a login and a password, specific to a User, allowing access to the Personal Area.
Issuer	Refers to the Institution issuing the Card to the Customer for a fee.
Manager	Refers to a natural person of legal age, appointed by the Customer, who is tasked with the management of a Team. They may in particular add new Employees to the team.
Monthly Plan	Means a Plan in which access to the Services is offered in exchange for a monthly subscription fee.
Network	Refers to the Mastercard payment processing network.
Owner	Refers to a natural person of legal age or emancipated minor, mandated by the Customer, having all the rights on the Account(s) including creating and closing it/them.
Password	Designates the secret code to access the Personal Area.
Payer	Refers to a legal or natural person who holds the Payment Account(s) and authorises a Payment Order from that Account.
Payment Account(s) or Account(s)	Refers to the Principal Payment Account and/or the Additional Payment Accounts opened in the Institution's books on behalf of the Customer for the purpose of providing the Payment Services.
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 services	Refers to the payment services provided by the Institution under the Contract. The Institution is authorised to provide services 2, 3, 5, 7 and 8 of Article L. 314-1, II of the Monetary and Financial Code.

Payment Transaction	Refers to a withdrawal or transfer of funds action executed by the Institution and charged to the Payment Account.
PEPPOL Service Provider	Refers to an entity providing Peppol Access Points (AP) and Service Metadata Publisher (SMP) services on the PEPPOL network.
Personalised Security Credential	Refers to the personalised data provided to a User by the Institution for authentication purposes. Personalised Security Credentials includes Identification Data as well as any data related to a Simple Authentication or Strong Authentication procedure defined by the Institution.
Personnel Area	Refers to the dedicated environment of the Customer (or a Customer-designated User) accessible via the Application or the Site using the Identification Data.
Plan	Means a fixed price determining the Services to be provided to the Customer, the price applicable to these Services and the billing frequency.
Principal Payment Account	Refers to the first payment account opened in the books of the Institution, on behalf of the Customer, to provide Payment Services. This account is identified as a principal account, on which the Institution invoices Payment Services.
Qonto	Refers to the brand under which the Institution markets the Services.
Services	Refers to all services provided by the Institution to the Customer under this Contract, including the Payment Services.
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 Credentials and Identification Data.
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 Transaction, the amount and the Beneficiary.
Subscription Fees	Refers to the flat fee charged periodically by the Institution for access to the Services under a Plan for the Customer.

Team	Refers to all of the Employees under the responsibility of the Manager.
Transaction Fees	Refers to the charges levied by the Institution in return for the performance of services or transactions offered by the Institution and not covered by the Customer's Plan. Transaction fees include, in particular, all fees related to the execution of a Payment Transaction, the use of a Card or Special Operations.
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, Employees and the Accountant are Users under a duly completed power of attorney.
Wallet Service	Service provided by a third-party provider that enables saving the Card details in a dedicated mobile application so as to carry out Card Payment Transactions from a mobile phone. The Cardholder will have previously approved saving these Card details.
Website	Refers to the website published and operated by the Institution to access the Personal Area.
Working Day	Refers to a calendar day with the exception of Saturdays, Sundays and public holidays in metropolitan France during which payment infrastructures and banks exercise their activities in regular operation.

Appendix 1 - Documents required to open a Payment Account

Any prospect wishing to create a Principal Payment Account must provide the Institution with the following information and documents:

Natural person

- Valid identity document

- If the Contract is signed by a person other than the corporate officer of the company: the attorney's proof of authority and proof of identity document

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

- Any other document required by the Institution for registration

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 proof of identity document

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

- Any other document required by the Institution for registration

Appendix 2 - Rights associated with each User

Category	Action	Owners	Administrators	Manager	Employees	Accountants
Activity	View transactions	yes (all)	yes (all)	yes (customisable)	yes (only their transactions)	yes (all)
	Export transactions	yes	yes	yes (dedicated team transactions only)	no	yes
Transfers	Initiate a credit transfer	yes	yes	yes (external only)	no	no
	Modify a credit transfer	yes	yes	yes	no	no
Cards	Create a card	yes	yes	yes (for dedicated team only)	no	no
	Set the PIN code of a card	yes (own card)	yes (own card)	yes (own card)	yes (own card)	no
	Block a card	yes (all cards)	yes (all cards)	yes (customisable)	yes (own card)	no
	Unblock a card	yes	yes	yes (customisable)	no	no
Accounts	Create the Principal Payment Account	yes	no	no	no	no
	Close the Principal Payment Account	yes	no	no	no	no
	Create the Additional Payment Accounts	yes	yes	no	no	no
	Close the Additional	yes	yes	no	no	no

	Payment Accounts					
	Download Account statements	yes	yes	yes	no	yes
	View the IBAN of the Principal Payment Account	yes	yes	yes (customisable)	no	yes
Team	Invite a User	yes	yes	yes (dedicated team only or an Employee)	no	no
	Revoke a User	yes	yes	yes	no	no
	Edit the address of a User	yes	yes	no	no	no
Parameters	Edit the information of the organisation	yes	no	no	no	no
	Enter a voucher	yes	yes	no	no	no
	Download invoices	yes	yes	no	no	no
Profile	Edit personal settings	yes (for themselves)	yes (for themselves)	yes (for themselves)	yes (for themselves)	yes (for themselves)
	Change email	yes (for themselves)	yes (for themselves)	yes (for themselves)	yes (for themselves)	yes (for themselves)
	Set authentication settings	yes (for themselves)	yes (for themselves)	yes (for themselves)	yes (for themselves)	yes (for themselves)
Request	Submit a transfer request	no	no	yes (customisable)	yes	yes
	Validate a transfer request	yes	yes	yes	no	no
Activity	View transactions	yes (all)	yes (all)	yes (customisable)	yes (only their transactions)	yes (all)

Qonto