Memo Bank

SERVICES AGREEMENT

General Terms and Conditions

Last updated on August 25, 2026

> **Unofficial translation.** This document is an unofficial English translation of Memo Bank’s Services Agreement (General Terms and Conditions and their schedules), the authoritative version of which is published in French at: https://memo.bank/convention.
>
> It is provided for information purposes only, as a courtesy to facilitate understanding; it has no contractual value of its own and creates no rights or obligations.
>
> In the event of any discrepancy, divergence of interpretation or conflict between this English translation and the French version, **the French version shall prevail in all respects.**

1. How to read this document

Memo Bank is committed to providing its customers with clear legal documents. We make every effort to simplify the reading and understanding of the contracts you sign. If any part of this text seems difficult to understand, please do not hesitate to contact us.

Terms we consider essential begin with a capital letter (for example: Account) and are defined in the glossary below. We also invite you to supplement your reading with our online help centre.

2. The services agreement

This services agreement is made up of three documents:

- the General Terms and Conditions and their schedules (the document you are now reading);
- the Special Terms and Conditions;
- the Fee Schedule.

This services agreement is referred to as the "Agreement" in this document for ease of reading.

The Agreement is entered into between "you", the legal entity identified in the Special Terms and Conditions, and "us", Memo Bank, a French *société anonyme* with an executive board and a supervisory board, with share capital of €13,494,482.33, registered with the Paris Trade and Companies Register under number 829 226 760, having its registered office at 50 avenue des Champs-Élysées, 75008 Paris, France. Memo Bank holds a credit institution licence and is supervised by the French Prudential Supervision and Resolution Authority (*Autorité de Contrôle Prudentiel et de Résolution* — ACPR), located at 4 place de Budapest, 75436 Paris Cedex 09.

This Agreement is entered into for an indefinite term.

We may amend this Agreement, including the Fee Schedule, at any time.

Most amendments serve to clarify or supplement certain points. In the event of a material amendment to the Agreement, you will be informed by email.

If you refuse such amendments, you may then terminate the Agreement in accordance with clause 19, “Termination”. If you do not react within one month, we will consider that you have accepted them.

Certain legal or regulatory provisions may require us to amend the Agreement.

The updated General Terms and Conditions and Fee Schedule are in any event available online at the following address: https://memo.bank/convention.

3. How we communicate with each other

We communicate by default in French. You may contact us:

- by email at contact@memo.bank;
- by post at the following address: Memo Bank, 50 avenue des Champs-Élysées, 75008 Paris, France.

We make this English translation of the services agreement available to you. It is provided for information purposes only. In the event of any divergence in interpretation or any dispute concerning the validity or performance of any of the clauses of the agreement, only the French version shall prevail.

4. Definitions

Acquirers	Natural or legal persons to whom payments are made by Card.
API	Application Programming Interface, which allows two IT systems to communicate and exchange data with each other.
Open Banking API	API allowing duly authorised third-party institutions to access banking data and initiate payments, in accordance with Directive (EU) n° 2015/2366, known as "PSD2".
Premium API	API enabling you to access data and documents stored in your Workspace and to carry out operations by connecting your own IT infrastructure to your Workspace.

Strong Customer Authentication	Procedure by which a User confirms their identity by entering their login credentials and password and performing an action via their personal mobile telephone.
Simple Authentication	Procedure by which a User confirms their identity by entering their login credentials and password.
Payee	Natural or legal person who is the recipient of a Payment Transaction.
Card	Visa payment card, either dematerialised (Virtual Card) or physical (Physical Card), linked to your Account.
Click to Pay	Online payment solution offered by Visa allowing purchases to be settled without manually entering Card details, by means of a secure digital profile associated with the Card.
Account	Bank account opened in your name on our books.
Booster Account	Account that is remunerated on a specific basis in accordance with the Fee Schedule.
Foreign Currency Account	Account held in an Eligible Currency other than the euro.
Special Account	Account subject to specific regulatory requirements, such as a special-purpose account or an escrow account. A Special Account must be the subject of a separate agreement.
Principal Account	First bank account opened in your name on our books.
Term Deposit Account	Account on which a single deposit is made and which earns interest provided that it remains locked for a fixed period.
Terms of Use	Schedule to the Agreement describing the conditions of use of Visa Physical Cards and Virtual Cards.
Special Terms and Conditions	Contract you sign under which you accept the application of all the terms of the Agreement and which may, where applicable, derogate from the General Terms and Conditions.
Fee Schedule	Document detailing all the fees applicable to the use of our services. The applicable Fee Schedule is the one specifically agreed in the Special Terms and Conditions or, in the absence of any specific agreement, the one displayed on our website (available at this address: https://memo.bank/convention).
Agreement	Contractual framework comprising these General Terms and Conditions (including their schedules), the Special Terms and Conditions and the Fee Schedule.
Value Date	Date used to record interest (credit or debit) on an Account.
Execution Date	Date on which a Payment Order is actually processed. The amount of the transaction is then debited from the account.

Unauthorised Overdraft	Debit balance of an Account not covered by an overdraft agreement.
Banking Solicitation	Any unsolicited contact, by any means whatsoever, with a specified natural or legal person, with a view to obtaining their agreement, in particular, to the provision of a payment service within the meaning of Articles L. 341-1 et seq. of the French Monetary and Financial Code, save for legal exemptions.
Eligible Currency	Any currency other than the euro accepted by Memo Bank and mentioned in the Fee Schedule or in your Workspace.
Personalised Security Credentials	Personalised data specific to each User and used for the purposes of Strong Customer Authentication or Simple Authentication.
EBICS	EBICS (Electronic Banking Internet Communication Standard) is a secure exchange protocol between financial institutions and their customers. This protocol exists in two variants: – EBICS-T, which requires confirmation of Orders; – EBICS-TS, in which Orders include an electronic signature sufficient for their validation.
Workspace	Online interface dedicated to a legal entity, to which each authenticated User has access.
SEPA Zone	The Single Euro Payments Area (SEPA) is a unified payment area put in place by the banks of several European countries to facilitate transactions in euros. This area comprises around thirty countries not all of which are part of the eurozone.
€STR	The €STR or *Euro Short-Term Rate* reflects the unsecured overnight funding costs in euros of banks located in the euro area. It is published on the European Central Bank's website, via its Market Information Dissemination (MID) platform and on the European Central Bank's data portal. This publication takes place on each TARGET2 Business Day at 08:00 CET based on transactions carried out and settled on the previous TARGET2 Business Day (the reporting date "T") with a maturity of T+1.
Euribor	The Euribor or *Euro InterBank Offered Rate* is a reference rate of the euro money market, administered by the *European Money Markets Institute*, calculated for five maturities: one week, one month, three months, six months and twelve months. It measures the average interest rate at which financial institutions lend money to each other on the euro-area interbank market. It is published on each TARGET2 Business Day at 11:00 CET by the *European Money Markets Institute*.
Eurosystem	Monetary authority of the euro area, comprising the European Central Bank and the national central banks of the Member States of the European Union that have adopted the euro.

IBAN	The IBAN (International Bank Account Number) is the international identifier of a bank account.
Virtual IBAN	Bank identifier linked to a principal account, used to carry out Payment Transactions debiting or crediting your Accounts while masking the main IBAN from your counterparty.
Integrator	Third-party technical service provider, which may also publish a software solution, acting as a technical intermediary for the routing of data flows and instructions between the Account Holder and Memo Bank. The Integrator at no time takes possession of the funds, exercises no control over them and does not provide a payment service in its own name, but is limited to providing infrastructure and the technical routing of data on behalf of the Account Holder.
Business Day	Day (other than a Saturday, Sunday or public holiday) on which the payer's or the payee's payment service provider carries on an activity making it possible to execute Payment Transactions, subject to the opening of the TARGET2 payment system for transactions in euros, or of the interbank systems of the relevant currency for transactions in foreign currencies.
Working Day	Calendar day corresponding to the customer-service opening hours indicated on the Website or on any other medium.
SEPA Core Direct Debit Mandate or B2B Direct Debit Mandate	A SEPA direct debit (SDD) mandate is a mandate given by a Payer to the Payee allowing the latter to carry out debit transactions in euros from the Payer's accounts in all countries within the SEPA Zone. It is a means of payment that may be used to collect recurring or one-off invoices from a debtor. There are two types of SDD mandates: – the Core Direct Debit Mandate: it applies to all types of debtors (whether consumers or businesses); – the B2B (business-to-business) Direct Debit Mandate: it is used exclusively between businesses and applies neither to consumers nor to sole traders.
Marketplace	Application directory listing third-party solutions and allowing the Account Holder to interconnect its Account and Workspace with the tools published by Partners.
MCP (Model Context Protocol)	Open protocol, published by the company Anthropic, defining the technical arrangements for standardised interaction between a client application (in particular an artificial-intelligence agent) and a third-party information system.
Memo Bank MCP Server	Interface implementing the MCP (Model Context Protocol) and exposed by Memo Bank, through which an Integrator or a Partner authorised by you may, in your name and on your behalf, within the limits of the authorisations you have granted to it, access your Workspace and execute therein the operations made available by Memo Bank.

Payment Transaction	One of the payment transactions we offer, detailed in clause 7, “Payment Transactions”.
Payment Order	Instruction given a) by the Payer, who gives a payment instruction to their Payment Service Provider (Payment Order by Credit Transfer or Payment Order by Card); b) by the Payee, who gives a payment instruction to the Payer's Payment Service Provider, based on the consent given by the Payer to the Payee and, where applicable, through their own Payment Service Provider (Payment Order by Direct Debit).
Partner	Any entity, whether an Integrator or a duly authorised payment service provider, whose solution is listed on the Marketplace.
Payer	Natural or legal person who gives or authorises a Payment Order.
Cardholder	Any person who uses a Card issued in their name, whether the Representative or a User.
Payment Initiation Service Provider	Service provider, authorised by an authority established in a Member State of the European Union or in a Member State of the European Economic Area, which provides a service consisting in initiating a Payment Order at the request of a User from an Account.
Account Information Service Provider	Service provider, authorised by an authority established in a Member State of the European Union or in a Member State of the European Economic Area, which provides a service, commonly referred to as "account aggregation", consisting in providing consolidated information concerning one or more accounts held by the Account Holder with one or more payment service providers.
Payment Service Provider	Credit institution, electronic-money institution or payment institution authorised by an authority established in a Member State of the European Union, in a Member State of the European Economic Area or in a third country imposing equivalent obligations regarding anti-money laundering and counter-terrorist financing.
Power of Attorney	Power given to another person to act in your name.
Profile	All the data associated with a User.
Representative	Natural person empowered to represent the Account Holder, who signs the Special Terms and Conditions of the Agreement in its name and on its behalf.
Services	Services we provide to you under this Agreement.
Website	Website accessible at https://memo.bank.
SWIFT	SWIFT (*Society for Worldwide Interbank Financial Telecommunication*) is a secure international network enabling financial institutions to exchange standardised financial messages, facilitating international payments.

TARGET2	Payment system belonging to the Eurosystem, which ensures its operation. It is the principal European platform for the processing of large-value payments, used both by central banks and by commercial banks to execute payments in euros in real time.
Account Holder	Legal entity (company) in whose name the Accounts are opened.
User	Representative and any person who has been granted a Power of Attorney to use a Workspace.
Verification of Payee	The Verification of Payee ("VOP") is a service used to confirm the matching of the IBAN and the name of the payee entered. This check applies only to SEPA Credit Transfers and SEPA Instant Credit Transfers.
Credit Transfer	Payment Transaction ordered by a Payer, who gives the order to transfer funds to their Payment Service Provider in favour of a Payee.
Bulk Credit Transfer	Single Payment Order comprising the simultaneous execution of a set of several individual Credit Transfers.
Standing Order	Credit Transfer that is executed automatically, on a recurring basis and at regular intervals, for a fixed or indefinite period.
International Credit Transfer	Type of Credit Transfer routed through the SWIFT network. It is mainly used where: – the Payer's or the Payee's Payment Service Provider is located outside the SEPA Zone; – the Credit Transfer is denominated in a currency other than the euro. Unlike a SEPA Credit Transfer, an International Credit Transfer gives rise to a commission charge in accordance with the Fee Schedule. When credited to your Account, it is credited at the latest on the fourth Business Day following the day of receipt of the Payment Order by Credit Transfer.
SEPA Credit Transfer	Type of Credit Transfer used where the Payer's and the Payee's Payment Service Providers are both located in the SEPA Zone.
SEPA Instant Credit Transfer	Officially called "SEPA Instant", "Instant Payment" or "SCT Inst", this is a type of Credit Transfer which, according to the European Payments Council, must be credited within a target time of less than 10 seconds from receipt, by the Payee's Payment Service Provider, of the Payment Order by Credit Transfer.
Standard SEPA Credit Transfer	Officially designated "SEPA Credit Transfer" or "SCT", the standard Credit Transfer is a type of Credit Transfer whose amount is credited at the latest on the Business Day following the day of receipt by the Payee's Payment Service Provider of the Payment Order by Credit Transfer. It may be either an immediate Credit Transfer or a scheduled Credit Transfer.

5. Access to our Services

5.1. Our Services

In consideration of the fees and commissions set out in the Fee Schedule, we provide the following Services:

- the holding of Accounts;
- the execution of Payment Transactions, detailed in clause 7, “Payment Transactions”.

Your Accounts and the Payment Transactions are denominated in euros (code: EUR) and in Eligible Currencies.

We provide these Services to you once all the documents required for your onboarding have been received and validated by Memo Bank. Additional Services to those listed above may be provided by Memo Bank: for the sake of clarity, they shall be the subject of separate agreements.

5.2. Annual commitment

Certain subscriptions are subject to an annual financial commitment (the "Commitment").

The Fee Schedule and your Special Terms and Conditions set out the amount and arrangements of the Commitment.

The Commitment relates exclusively to subscription fees and commissions. It does not prevent variation of the credit interest rates applicable to deposits, which remain governed by the conditions set out in clause 5.5, “Remuneration of your deposits”.

5.2.1. Principle: usage-based billing, Commitment smoothed over 12 months

By subscribing to an offer with a Commitment, you guarantee a minimum annual amount of subscription fees and commissions (excluding foreign-exchange fees) over a period of 12 consecutive months (hereinafter the "Commitment").

The amount and the effective date are set out in your Special Terms and Conditions.

5.2.2. Billing mechanism

Invoicing is established monthly in accordance with the following rule:

At the end of each month, we calculate:

- (A) the cumulative amount of your actual usage (comprising subscription fees and commissions, hereinafter the "Usage") since the beginning of the Commitment period;
- (B) the portion of the Commitment corresponding to the number of days elapsed since its effective date: annual Commitment × (number of days elapsed ÷ 365) (or 366 in leap years).

The amount invoiced for the month is equal to the difference between:

- the higher of (A) and (B); and
- the total already invoiced in previous months.

For example, for a Commitment of €12,000 taking effect on 15 January, the portion due as at 31 January (17 days) is: €12,000 × 17 ÷ 365 = €559.

5.2.3. Practical consequence

- In months where your cumulative Usage is lower than the due portion of the Commitment, you pay this portion: the difference constitutes a prepaid balance (hereinafter the "Prepaid Balance").
- In the following months, if your cumulative Usage exceeds the due portion, this Prepaid Balance absorbs the surplus.
- Once the Prepaid Balance has been exhausted, you pay your actual Usage.

If, at the end of the relevant period, your cumulative Usage remains lower than the amount of the Commitment, the difference (the remaining Prepaid Balance) shall remain definitively acquired by Memo Bank.

It shall not give rise to any refund or to any carry-over to the following year.

5.2.4. Amendment, renewal and termination

Amendment of the Commitment

You may request to amend the amount of your Commitment at any time. Such amendment entails:

- the immediate closing of the current period; and
- the opening of a new 12-month period with the counters reset to zero.

If, on the date of amendment, the total amount invoiced exceeds your actual Usage, the difference shall remain acquired by Memo Bank and shall not give rise to any refund or carry-over.

Renewal

Upon its expiry, the Commitment shall be renewed by tacit renewal for 12 months, on the same fee terms.

Either party may object to such renewal by notifying the other in writing at least one month before the expiry of the current period.

Early termination

In the event of termination or closure of your Account before the expiry of the Commitment, you shall remain liable for the higher of the following amounts:

- the portion of the Commitment pro rata to the time elapsed; or
- your actual Usage.

By way of exception, this portion of the Commitment is not due if termination follows your refusal of an amendment to the Agreement, whether you choose to close your Account or switch to a fee structure without a Commitment.

5.3. Your Accounts

The balance of each of your Accounts must at all times be positive or equal to zero. It is therefore your responsibility to maintain a sufficient balance to ensure the proper execution of Payment

Transactions. For the same reason, we refuse to execute any Payment Transaction that would result in the balance of one of your Accounts becoming negative.

We make account statements available to you in your Workspace each month or at any other frequency specified in the Special Terms and Conditions. Each statement details the transactions carried out on an Account, recorded in the order in which they are actually presented to us. You must verify the accuracy of the information on the account statements upon receipt.

You may also have your account statements sent in MT940 format via the SWIFT network. Configuring the dispatch of account statements in this format is your responsibility. It is therefore up to you to ensure that the Bank Identifier Code (BIC) of the recipient of these statements is correctly entered.

In the event of an unauthorised debit balance on an Account, we charge you interest at the rate applied to unauthorised overdrafts, in accordance with our current Fee Schedule. We draw your attention to the fact that interest due for a whole year will itself bear interest (application of Article 1343-2 of the French Civil Code). The sums of such interest may be claimed at any time and must be paid in full.

5.4. Use of Virtual IBANs

The Virtual IBAN is a routing identifier linked to the Account of which you are the Account Holder.

It does not have a separate holder. Any Payment Transaction initiated or received by means of a Virtual IBAN takes effect directly on the Account to which it is linked and binds you as if it had been carried out using the primary IBAN of that Account.

When you provide a Virtual IBAN to a third party, your name as it appears on our books must be included as the account holder. You may add an additional reference, provided that it does not suggest that the account is held by a person other than yourself.

You are solely responsible for your use of Virtual IBANs and for ensuring that such use complies with the laws and regulations applicable to you.

5.5. Remuneration of your deposits

The credit balance of certain of your Accounts, such as the Booster Account, Term Deposit Accounts or Special Accounts, may be remunerated, at a credit interest rate and on terms set out in the applicable Fee Schedule.

The remuneration rate is an annual rate, on the basis of a 360-day year, calculated daily by reference to:

– the lowest credit balance recorded during a single day on the Account;

– the latest €STR rate published by the European Central Bank.

Remuneration on your Accounts is paid to you once a month on your Principal Account.

Remuneration on the Booster Account is paid to you once a month on the Booster Account.

Interest is subject to the social charges and taxation applicable to this type of product.

In the event of unavailability or disappearance of the €STR, we will use the substitute index retained by the competent authorities (or any entity designated by the competent authorities).

In the absence of a substitute index, we will use the three-month Euribor.

The remuneration of your deposits may be amended unilaterally at any time, in particular in the event of a decrease in the European Central Bank's key rates, of regulatory developments, or for specific reasons relating to our relationship and to the management of our balance sheet. Any such amendments will be available on our help website and in your Workspace.

5.6. Your Booster Account

5.6.1. Opening of the Booster Account

The opening of a Booster Account is free of charge provided that you already hold an Account.

You may open a single Booster Account by accessing the Workspace.

5.6.2. Operation of the Booster Account

No Payment Transaction by Card or by direct debit may be carried out from the Booster Account.

5.7. Your Term Deposit Accounts

5.7.1. Opening of a Term Deposit Account

The opening of a Term Deposit Account is free of charge provided that you already hold an Account.

You may open one or more Term Deposit Accounts by accessing the Workspace, where you will be able to choose the amount you wish to deposit in each Term Deposit Account, as well as its term. You will then be invited to sign electronically a contract setting out the characteristics of the Term Deposit Account.

As market conditions are subject to change, you have a 24-hour period to sign this contract and validate the remuneration terms of your Term Deposit Account.

The signing of this contract automatically entails the payment of the amount you have chosen into the Term Deposit Account.

We draw your attention to the fact that:

– the minimum amount that may be deposited into a Term Deposit Account is €5,000; if the credit balance of your Account is insufficient to make a deposit of this amount into a Term Deposit Account, the opening of the latter will not be possible;

– the maximum cumulative amount that may be deposited into all the Term Deposit Accounts you may open is €10 million; any deposit exceeding this amount must be the subject of our express agreement;

– only a single deposit may be made per Term Deposit Account: if you wish to make an additional deposit, you must open a second Term Deposit Account, and so on.

5.7.2. Remuneration of the Term Deposit Account

The remuneration applicable to a Term Deposit Account varies according to the length of time for which you block the deposited sums. It is specified in the Workspace.

This remuneration is progressive and increases at the end of:

– a period of three months from the opening of your Term Deposit Account;

- a period of six months from the opening of your Term Deposit Account;
- the first year, and then each subsequent year.

Depending on the length of time for which you block the funds in a Term Deposit Account, the interest generated by the sums deposited is automatically paid into the Account of your choice, first after a three-month period, second after a six-month period, third after a one-year period, and then every year.

5.7.3. Maturity of the Term Deposit Account

At the end of the term you chose when opening the Term Deposit Account, the sums recorded therein and any interest still owed to you will be automatically transferred to your Account.

5.7.4. Early withdrawal of sums deposited in the Term Deposit Account

You may withdraw all or part of the sums recorded in the Term Deposit Account before the expiry of the term chosen when opening it, subject to giving 32 days' notice.

In such case, the interest generated by the sum you have withdrawn will be calculated according to the effective period during which it was deposited in the Term Deposit Account.

In the event of a partial withdrawal, this interest will be automatically paid into your Account at the end of the current period. For example, if you withdraw the sums recorded in the Term Deposit Account four months after its opening, the interest will be paid to you at the end of the sixth month.

5.8. Automatic treasury management rules

Within your Workspace, you may, at your sole discretion, set up automated treasury management rules and enable or disable them at any time. These rules trigger the execution of transactions based on predetermined criteria.

They allow you to:

- schedule automated or conditional Transfers between your various Accounts, including to or from your Booster Account;
- set up automated subscription or redemption orders for financial instruments, executed from your Booster Account as soon as certain criteria are met; setting up these orders requires that you have accepted the general terms and conditions for investment services and have previously received a suitability statement.

Each transaction scheduled in this manner is executed solely on the basis of your settings and does not constitute a personal recommendation on our part, nor a reception and transmission of orders (RTO) service.

You retain full control over your treasury and act at your own risk and responsibility.

Consequently, we shall not be held liable for any financial losses, liquidity shortfalls, differences in returns, or lost profits resulting from the execution of the rules you have configured, whether involving Transfers between your Accounts or transactions in financial instruments.

5.9. Foreign Currency Accounts

The opening of a Foreign Currency Account is subject to our express and prior agreement. We reserve the right to accept or refuse any opening request on the basis of objective criteria relating, in particular, to your activity, your risk profile or our operational constraints, without incurring any liability. Such agreement may be revoked subject to a reasonable notice period and subject to the processing of any pending Payment Transactions.

Each currency is the subject of a separate Account. If you open several Accounts in the same currency, they are grouped together and treated as a single Foreign Currency Account.

The following restrictions apply to your Foreign Currency Accounts:

- you may not deposit or withdraw cash;
- no Payment Transaction by Card or by direct debit may be carried out from a Foreign Currency Account;
- any currency conversion generates a foreign-exchange risk that you bear.

5.9.1. Removal of a currency from the list of Eligible Currencies

If a currency is removed from the list of Eligible Currencies, we will inform you by email as soon as possible, indicating the date as from which that currency may no longer be used.

As from that date, no new Payment Order debiting or crediting the relevant Foreign Currency Account may be executed. You may close the relevant Foreign Currency Account in accordance with the arrangements described in clause 5.9.3, “Closure of a Foreign Currency Account”.

5.9.2. Outgoing Credit Transfers from a Foreign Currency Account

Payment Orders by Credit Transfer issued from a Foreign Currency Account are processed in accordance with the provisions applicable to International Credit Transfers, subject to the following adjustments:

- if the Payee holds an account denominated in the same currency as the Foreign Currency Account being debited, no conversion is carried out and the amount is transmitted in that currency;
- if the Payee’s account is denominated in a different currency, the conversion is carried out at the reference exchange rate in force on the day of processing, with application of the foreign-exchange fees provided for in the Fee Schedule;
- you bear the entirety of the foreign-exchange risk resulting from any fluctuation in the rate between the date of transmission of the Payment Order and its actual execution date.

The time limits, refusal conditions and revocation arrangements applicable to International Credit Transfers apply fully to Payment Orders issued from a Foreign Currency Account.

5.9.3. Closure of a Foreign Currency Account

You may request the closure of a Foreign Currency Account at any time, independently of any termination of the Agreement, from your Workspace.

The closure takes effect provided that all pending Payment Transactions or Payment Transactions awaiting execution debiting or crediting the Account have been fully processed and that no protective attachment, garnishment or similar enforcement measure is encumbering the relevant Account.

On closure, you choose in your Workspace to:

- transfer the balance to another Foreign Currency Account that you hold in the same currency on our books, without conversion or fees;
- transfer the balance to an external account denominated in the same currency, by International Credit Transfer, in accordance with the Fee Schedule;
- convert the balance into euros and credit it to your Principal Account, at the reference exchange rate in force on the day of conversion, with application of the foreign-exchange fees provided for in the Fee Schedule.

5.10. Users — Power of Attorney

When the Principal Account is opened, only the Representative may access the Workspace and use the Services. However, the Representative may grant a Power of Attorney to one or more Users to access the Workspace and carry out actions in your name and under your responsibility.

The rights defined by the Representative for each User define and limit the actions permitted to the User within the Workspace. Depending on the rights granted by the Representative to the User, the User may themselves grant a Power of Attorney to other Users to access the Workspace and carry out actions in your name and under your responsibility.

Transactions initiated by Users on the Accounts bind you as if you had carried them out yourself.

The Power of Attorney must be granted by the Representative or by an authorised User within the Workspace, where the steps to be followed are specified. We reserve the right not to approve a User or to revoke its approval at any time, without prior notice or justification, without such decision giving rise to any liability on our part.

Any User may at any time revoke a Power of Attorney granted, directly or indirectly, in the Workspace.

The Representative may also grant a Power of Attorney to a third-party application listed on the Marketplace.

By activating such connection, the Representative grants the Partner a mandate to transmit Payment Orders and to retrieve data in the name and on behalf of the Account Holder via the Premium API or the Memo Bank MCP Server.

Instructions and Payment Orders transmitted through a Partner bind you as if you had carried them out yourself.

5.11. Users — Mobile telephone

Each User must hold a mobile telephone equipped with the iOS operating system (version 12 or later) or Android (version 6 or later).

5.12. Personalised Security Credentials

Every User receives Personalised Security Credentials specific to them, which allow access to the Workspace by means of a Strong Customer Authentication or Simple Authentication procedure, as the case may be.

You undertake to take all necessary steps to ensure that each User preserves the confidentiality and security of the Personalised Security Credentials assigned to them.

In any event, you remain liable for the consequences of any disclosure of the Personalised Security Credentials and their use by third parties, for example by a Payment Initiation Service Provider or an Account Information Service Provider.

In the event of loss or theft of the Personalised Security Credentials, or in the event of any misappropriation or unauthorised use of the Workspace, you undertake to inform us without delay by email at the following address: contact@memo.bank. This enables us in particular to immediately block access to your Workspace and to handle any dispute regarding Payment Transactions in accordance with the conditions described in clause 7.8, "Dispute of a Payment Transaction".

5.13. Workspace

Our Services are provided via a Workspace, to which each User has access by means of their Personalised Security Credentials.

In order to guarantee the security of your Accounts, no Payment Transaction may be initiated, validated or refused through your Workspace except by following the instructions given to you.

Likewise, the use of all the features ancillary to the management of your Accounts that we make available to you, such as pre-accounting tools or the extraction of VAT information from receipts and invoices, requires the instructions given to you in the Workspace to be followed.

We of course do our utmost to ensure maximum availability of the Workspace. However, the Services may be temporarily interrupted for technical reasons.

Finally, in the event of a security incident or suspicion of unauthorised or fraudulent use of your Workspace, including through an Account Information Service Provider, a Payment Initiation Service Provider or any other Partner, we may block access to it. In such case you will be informed as soon as possible and by any means, unless the law or an overriding security requirement prevents us from doing so. Depending on the situation, we may require the Personalised Security Credentials of Users to be reset before unblocking access to the Workspace.

5.14. Marketplace and third-party tools

Memo Bank offers a Marketplace allowing you to link your Account and your Workspace with third-party tools (accounting, treasury, CRM, etc.) published by Partners.

These Partners may be technical service providers or authorised institutions such as Account Information Service Providers or Payment Initiation Service Providers.

By activating a tool from the Marketplace, you give us express instruction to:

– transmit to the Partner the data of your Accounts and your transactions;

- receive and execute the instructions (including Payment Orders) transmitted by the Partner via the Premium API or the Memo Bank MCP Server.

The use of these third-party tools is subject exclusively to the contractual terms of the relevant Partner.

Memo Bank acts as a platform for connecting and transporting data but exercises no control over the operation, algorithms or security specific to the Partner's tools.

We shall not be liable for:

- the consequences of the execution of a Payment Order we received from the Partner within the scope and limits of the authorisations you granted to it and that were in force at the time of transmission of the Order;
- any damage having its cause in a processing error, malfunction, unavailability or security breach attributable to the Partner or its subcontractors;
- any financial loss or erroneous decision resulting from an inaccurate interpretation, an erroneous summary or a "hallucination" generated by the Partner's tool (in particular the artificial-intelligence agents connected via the Memo Bank MCP Server) from the data we transmitted to it. In the event of any discrepancy, the data displayed in your Workspace shall alone be authoritative.

You may revoke a Partner's access at any time from your Workspace.

5.15. Suspension of the Services

We may temporarily suspend, in whole or in part, access to your Workspace, the use of the Services or the operation of all or part of your Accounts, in particular in the following cases:

- suspicion of fraudulent or unauthorised use, or use contrary to the Agreement;
- suspicion or risk of a breach of the security of your Workspace, your Personalised Security Credentials or our systems;
- breach by you of any of your contractual obligations, in particular those related to the provision of information or supporting documents;
- need to carry out checks as part of our know-your-customer or anti-money laundering and counter-terrorist financing obligations;
- request from a competent authority;
- any other reason relating to security, fraud prevention or our risk-management policy.

Unless prohibited by law or by an overriding security requirement, we will inform you of the suspension as soon as possible. The suspension ends when the reasons for it have ceased. The suspension does not entail termination of the Agreement and may not give rise to any liability on our part, nor confer any right to compensation in respect of transactions that could not be executed during that period.

6. Communication and updating of your data

Throughout the term of the Agreement, you undertake to:

- inform us without delay of any change in the information concerning you, provided at the time of onboarding or subsequently; you shall produce supporting documents which we shall check and which shall in particular relate to:
  - any change of address, telephone number or email address;
  - any change to your articles of association, change of company officer, change in the breakdown of the share capital among the partners or shareholders, or own funds that have become less than half of the share capital as a result of losses;
  - any amendment, loss, withdrawal, suspension or non-renewal of an authorisation, approval, licence, registration in a professional register, financial guarantee, regulated surety, or any other compulsory insurance required for the conduct of your activity;
  - any decision of merger, demerger, absorption, dissolution or voluntary liquidation;
  - any declaration of suspension of payments or court ruling opening insolvency proceedings;
- use the Workspace exclusively to designate, modify or revoke the Representative or any User. No other means of designating, modifying or revoking a User shall be accepted;
- provide us each year, as soon as possible and within 6 months following the end of each financial year, with your financial statements (balance sheet, income statement and notes) and, where applicable, the reports of your statutory auditor;
- provide us, where we so expressly request, with all documents and information on your economic, accounting and financial situation; in this respect, you shall in particular provide us with any document required by the regulations arising from international agreements concluded between France and the States of the Organisation for Economic Co-operation and Development (OECD) as well as with the United States in the context of the fight against tax fraud and tax evasion; these regulations, known as "CRS" (Common Reporting Standard) and "FATCA" (Foreign Account Tax Compliance Act), require banks to provide tax authorities with information relating to financial assets held by their customers abroad; accordingly, you must complete and submit to us, each time we send them to you, "self-certification" forms attesting to your tax residence and including, depending on the case, information about your beneficial owners;
- inform us of any change likely to affect your tax position or, where applicable, that of your beneficial owners, it being noted that, in such case, you will be required to complete a new self-certification form;
- inform us without delay of any event (whatever its nature, cause or origin, including any judicial, arbitral or administrative proceedings brought against you) materially and adversely affecting, immediately or in the future, a) your financial or legal situation, your assets or your business or b) your ability to meet your payment obligations.

7. Payment Transactions

We process several types of Payment Transactions. These Payment Transactions are initiated by Payment Orders, whether external or internal.

You undertake to communicate to us as soon as possible all the information we need to check Payment Transactions, whether recorded or upcoming. Such information may concern, among other things, the nature, destination and origin of these Payment Transactions. These checks are necessary to fight against money laundering and terrorist financing. Following these checks, we may decide not to execute the Payment Transaction in question, or even to terminate the Agreement.

Notwithstanding the reasons specifically mentioned in the clauses below, we reserve the right, at our sole discretion, to refuse, suspend, defer or cancel the execution of any Payment Transaction, whether crediting or debiting your Account, for any reason relating in particular to the security of the transaction, fraud prevention, our risk-management policy, your profile or any legal or regulatory obligation that may apply to us. Such decision shall not give rise to any liability on our part, nor confer any right to compensation. Unless prohibited by law, we will inform you of the reason for the refusal or deferral as soon as possible.

7.1. Caps applicable to Payment Transactions

Subject to the regulatory caps that apply to us and to you, we set caps applicable to the different types of Payment Transactions, whether carried out crediting or debiting your Accounts.

We reserve the right, at our sole discretion, to set, modify or remove these caps at any time, upwards or downwards, in particular having regard to your activity, your risk profile or our operational constraints. Any modification will be notified to you via your Workspace or by any other appropriate means.

7.2. Receipt of Payment Orders by Credit Transfer crediting an Account

7.2.1. Execution time of Standard SEPA Credit Transfers

We receive Payment Orders by Standard SEPA Credit Transfer in euros intended for you, and credit them to the target Account at the latest on the Business Day following the day of receipt.

We may reject or defer a Credit Transfer intended for one of your Accounts if the mandatory and regulatory information that must appear on the Payment Order by Credit Transfer transmitted by the payment service provider of the originator of the Credit Transfer is incomplete or invalid, or by reason of legal and regulatory obligations — in particular those relating to the fight against money laundering and terrorist financing.

If the Payer’s Payment Service Provider requests the cancellation of a Credit Transfer that was intended for you and that has been credited to your Account, we may, in the event of fraud or error — for example if a Credit Transfer was made twice by the Payer — debit your Account by the amount of that Credit Transfer and return the funds to the Payer’s Payment Service Provider.

7.2.2. Execution time of SEPA Instant Credit Transfers

Subject, on the one hand, to the Payment Order by Credit Transfer in euros intended for you originating from a Payment Service Provider in a position to execute it and, on the other hand, to the Payer having chosen to make a SEPA Instant Credit Transfer crediting your Account, we credit it within a target time of ten seconds from the receipt of the Payment Order.

We may reject a SEPA Instant Credit Transfer intended for one of your Accounts if the mandatory and regulatory information that must appear on the Payment Order by Credit Transfer transmitted by the originator's payment service provider is incomplete or invalid, or by reason of legal and regulatory obligations — in particular those relating to the fight against money laundering and terrorist financing.

If the Payer's Payment Service Provider requests the cancellation of a SEPA Instant Credit Transfer that was intended for you and that has been credited to your Account, we may, in the event of fraud or error, debit your Account by the amount of that Credit Transfer and return the funds to the Payer's Payment Service Provider.

7.2.3. Execution time of International Credit Transfers

We receive Payment Orders by International Credit Transfer intended for you, and credit them to the target Account at the latest within four Business Days following the day of receipt.

We may reject or defer an International Credit Transfer intended for one of your Accounts if the mandatory and regulatory information that must appear on the Payment Order by Credit Transfer transmitted by the Payment Service Provider of the originator of the Credit Transfer is incomplete or invalid, or by reason of legal and regulatory obligations — in particular those relating to the fight against money laundering and terrorist financing.

7.3. Issuance of direct debits crediting an Account

7.3.1. Setting up a Core or B2B Direct Debit Mandate

In order to set up a direct debit on the account of one of your debtors, you must:

1. Hold a SEPA Creditor Identifier (ICS)

If you already hold such an identifier, it is your responsibility to communicate it to us. Furthermore, under the regulations, you may hold only one ICS for all your outgoing direct debits within the SEPA Zone.

If you do not hold an ICS, you may ask us to request one on your behalf from the Banque de France. This service will then be invoiced to you in accordance with the Fee Schedule in force.

We draw your attention to the fact that, where the Banque de France indicates that an ICS has already been allocated to you, it will refuse your request and you will nevertheless have to pay the ICS allocation fees (which the Banque de France invoices us in all cases).

2. Set up a Direct Debit Mandate

You will find Core and B2B Direct Debit Mandate templates in the Workspace.

In this respect, you must in particular indicate a unique mandate reference ("UMR"). This is a code, of up to 35 characters, that you can establish freely and that identifies the mandate used for each direct debit.

Any direct debit on the account of your debtor also requires knowing their IBAN.

More generally, all the information requested in the mandate must be completed.

If any of this information is missing or incorrect, it will not be possible to carry out a direct debit.

You must also inform us of any change relating to the debtor, such as a change of address or trade name, so that we can determine whether the mandate is capable of being updated.

3. Have the Direct Debit Mandate signed by your debtor

To have the Direct Debit Mandate signed by your debtor, you may, at your discretion, use a third-party electronic signature solution, whether simple, advanced or qualified, or use the electronic signature solution offered by Memo Bank in the Workspace.

By signing the Direct Debit Mandate using the electronic signature solution offered by Memo Bank in the Workspace, your debtor and you will be deemed to have agreed that:

- the electronic signature used is a reliable authentication method which guarantees its link with the Direct Debit Mandate to which it relates;
- the electronic signature is evidence of the unequivocal consent of both you and your debtor to the stipulations, obligations, information, data, facts and elements contained in or arising from the direct debit mandate;
- in the event of a dispute, this electronic signature shall constitute valid and admissible evidence before all competent courts and authorities and vis-à-vis any third party;
- the electronically signed Direct Debit Mandate shall produce the same legal effects as a handwritten signed Direct Debit Mandate.

4. Inform your debtor that

- if they have signed a B2B Direct Debit Mandate, they must provide a copy thereof to their own Payment Service Provider. Without that copy, the Payment Service Provider must reject your direct debits;
- they may contact you at the contact details you indicate to them if they wish to amend, revoke or contest an existing SEPA Direct Debit Mandate;
- they may request the refund of the amount of a Core direct debit without justification even where it was validly authorised;
- they cannot request the refund of the amount of a validly authorised B2B direct debit.

5. Inform the debtor of the upcoming direct debit(s)

Unless you have agreed a different timeframe with your debtor, you must notify them at least 14 calendar days before the date on which the direct debit will be carried out on their account.

This notification may be made by any means of your choice, such as an invoice, a payment schedule or a direct debit notice. It must, however, always specify your ICS, the UMR, as well as the amount and date of the direct debit.

6. Transmit to us a Payment Order by direct debit with all the information relating to the Direct Debit Mandate

To issue a Payment Order by direct debit, the User must identify themselves in the Workspace, follow the instructions and correctly enter the information relating to the Payment Order by direct debit (debtor’s identity, IBAN, Execution Date, etc.).

This information must be entered correctly, in your name and under your responsibility. In particular, you must ensure that the account identified by the IBAN entered is indeed held by the debtor who signed the Direct Debit Mandate. We do our best to detect errors or fraud but we are not liable for them.

A User authorised to issue direct debit Orders from the Workspace may also do so from the EBICS client. Such direct debit Orders will then be processed in accordance with the information indicated in the direct debit files.

In all cases, direct debit Orders must be sent to us 2 Working Days before the date of presentation of the direct debit.

7. Retain the mandate

We disclaim all liability with respect to the retention of Direct Debit Mandates that have not been signed using the solution offered in the Workspace.

You must retain your Core or B2B Direct Debit Mandates for a minimum period of 13 months.

This is the maximum period within which your debtor may dispute a direct debit that has been defectively executed or that they did not authorise.

However, we recommend retaining the mandate for longer because, on top of these 13 months, there is a further period during which your debtor's Payment Service Provider may seek evidence of their consent to the direct debit in question.

We also draw your attention to the fact that, in accordance with the regulations, the debtor's Payment Service Provider may request, at any time, a copy of the Direct Debit Mandate.

8. Manage any dispute that may arise with your debtor

Even if, in certain circumstances, we are required to return sums that have been debited from your debtor's account, we are not liable for any disputes that may arise with them as to the sums owed to you under a Direct Debit Mandate.

We remind you in this respect that, in accordance with the regulations, any dispute of a direct debit does not affect the existence of your debtor's debt.

7.3.2. Processing of Core and B2B direct debits

We send Payment Orders by direct debit to your debtor's Payment Service Provider at the latest one Business Day before the agreed date of the direct debit.

It is then for the Payment Service Provider to execute the Payment Order by direct debit so as to enable your Account to be credited on the agreed date.

In your Workspace, you may arrange for Payment Orders by direct debit to be automatically retried if they are rejected, which may be the case if your debtors' account balance is insufficient or for the reasons described in our online help.

Such retries do not modify the existing invoicing rules: any rejected direct debit, whether or not it gives rise to an automatic retry, is invoiced and any retry is counted as an additional transaction in accordance with the Fee Schedule.

7.3.3. Suspension, revocation and lapse of Core or B2B direct debits

You must inform us from your Workspace if you wish to stop debiting your debtor. In such case, we suspend the Payment Orders by direct debit that have not yet been transmitted to your debtor's Payment Service Provider.

Likewise, you will no longer be able to carry out direct debits on your debtor's account where the latter revokes their consent and thereby terminates the Direct Debit Mandate. The revocation of the Core or B2B Direct Debit Mandate by your debtor may take place, at the latest, one Working Day before the direct debit date.

In addition, a Direct Debit Mandate that has not been used for more than 36 months automatically lapses.

7.3.4. Request for return of a validly authorised Core or B2B direct debit

The regulations require us to accept, for any SEPA direct debit, requests for the return of direct debits submitted by the debtor's Payment Service Provider, in particular in the event of insufficient funds:

- within three Working Days after a settlement made on the basis of a B2B direct debit;
- within five Working Days after a settlement made on the basis of a Core direct debit.

In such cases, we are required to return the amount debited and to debit your account accordingly. Furthermore, in accordance with the Fee Schedule, fees apply to such a transaction.

7.3.5. Request for refund of a validly authorised Core direct debit

Within a period of eight weeks — to which are added two Working Days of processing — from the date of a SDD Core direct debit, your debtor may request the refund of that direct debit from their Payment Service Provider.

In such case, we are required to return the amount debited and to debit your account accordingly. Furthermore, in accordance with the Fee Schedule, fees apply to such a transaction.

7.3.6. Dispute of an unauthorised or defectively executed Core or B2B direct debit

For a period of 13 months from the debit to their account, your debtor may dispute a direct debit that has been defectively executed or that they did not authorise.

In this respect, you undertake to:

- reply within a maximum of 7 Working Days to any request from us following a claim made by your debtor or their Payment Service Provider seeking the return of a direct debit;
- refund to us any sum due to your debtor's Payment Service Provider where we are required to grant a request to cancel a direct debit.

7.3.7. Setting up of guarantees

In accordance with the regulations, in particular with the rules established by the European Payments Council on direct debits — and as set out in clause 7.3.5, "Request for refund of a validly authorised Core direct debit", in clause 7.3.4, "Request for return of a validly authorised Core or B2B direct debit" and in clause 7.3.6, "Dispute of an unauthorised or defectively executed Core or B2B direct debit" — we may be required to return, to the Payment Service Providers of your debtors, direct debits made on the accounts of those debtors, whether validly authorised or not, with you remaining liable to refund these sums to us.

However, the more significant the number and amount of your direct debits, whether current or anticipated, the greater our exposure to the risk of having to return substantial sums to the Payment Service Providers of your debtors, even where the balance of your Accounts would be insufficient to repay us.

Similarly, the higher the proportion of refund, return or cancellation requests for direct debits made by your debtors or their Payment Service Providers, the greater our exposure to this risk.

This is the reason why we set a maximum amount of direct debits that may be carried out on the accounts of your debtors according to your risk profile.

In addition to this cap, which we may set or amend at any time, we reserve the right, at our sole discretion and irrespective of the thresholds mentioned below, to require the setting up of any guarantee measure that we deem necessary in light of the volume, nature or risk profile of your outgoing direct debits.

We may at any time put an end to existing measures, require additional measures or amend their arrangements, without such decisions giving rise to any liability on our part.

By way of indication, depending on your situation, such measures may be the following:

- if the proportion of refund, return or cancellation requests for direct debits represents between 1% and 3% of the number or total amount of direct debits you carry out, we may require you to keep your Accounts above a minimum credit balance; if you do not keep the credit balance of your Accounts above this threshold for more than five Working Days, we may deactivate the use of any outgoing direct debit feature;

- if the proportion of refund, return or cancellation requests for direct debits represents between 3% and 7% of the number or total amount of direct debits you carry out, we may require, at our discretion, the constitution of a cash collateral which may take one of the following forms:

    - either the delivery of a lump-sum amount as a guarantee, which will be returned to you if the proportion of the aforementioned requests falls durably below the 3% threshold or if you cease to use outgoing direct debits;

    - or the delivery of the amount of each direct debit received as collateral; the funds thus posted as collateral will be retained for a period of up to 10 Working Days, before being returned to you by being made available on your Account;

- if the proportion of refund, return or cancellation requests for direct debits exceeds 7% of the number or total amount of direct debits you carry out, we may deactivate any receipt of Payment Orders by Credit Transfer crediting your Accounts.

7.4. Issuance of Payment Orders by Credit Transfer debiting an Account

7.4.1. Consent

To execute a Credit Transfer, you must transmit a Payment Order to us. After identifying yourself in your Workspace, you must follow the Credit Transfer issuance procedure:

- you must correctly enter all the information relating to the Payment Order (Payee's identity, IBAN, Execution Date, etc.);

- this data must be entered correctly, in your name and under your sole responsibility. It is essential to ensure that the destination account, identified by the IBAN entered, is indeed held by the designated Payee. In this respect, we systematically carry out Verification of Payee (VOP);

- you must then confirm the Payment Order, after validation by Simple Authentication or Strong Customer Authentication, as the case may be.

If we detect a mismatch between the payee's name and IBAN, we will inform you. If you disregard this alert and validate the Credit Transfer, you risk losing any right to a refund.

In addition to the transmission of Payment Orders by Credit Transfer from the Workspace, we also accept the transmission of Payment Orders by SEPA Credit Transfer via an EBICS connection or via a Payment Initiation Service Provider.

Your consent results from the confirmation of the Payment Order by Credit Transfer.

7.4.2. Execution of SEPA Instant Credit Transfers

The execution of a SEPA Instant Credit Transfer debiting your Account is proposed by default in the Workspace, provided that the Payee's Payment Service Provider is in a position to accept this type of Credit Transfer.

Once the Payment Order by SEPA Instant Credit Transfer has been validly transmitted, we credit the account of the Payee's Payment Service Provider within a target time of ten seconds — which may extend up to twenty seconds in the event of technical difficulty — from receipt of the Payment Order.

If this twenty-second period is exceeded, the Payment Order by SEPA Instant Credit Transfer will not be taken into account and will be automatically cancelled. You will then need to send a new Payment Order.

A SEPA Instant Credit Transfer may be executed on any day and at any time. It does not need to be made on a Business Day.

The amount of a SEPA Instant Credit Transfer may not exceed the maximum amount applicable to your other Credit Transfers, nor the maximum amount provided for by the regulations.

We may refuse to execute a Payment Order by SEPA Instant Credit Transfer transmitted if the mandatory and regulatory information that must appear on the order is incomplete or invalid, or by reason of legal and regulatory obligations — in particular those relating to the fight against money laundering and terrorist financing.

7.4.3. Execution of Standard SEPA Credit Transfers

Once the Payment Order by Standard SEPA Credit Transfer has been validly transmitted, we credit the account of the Payee's Payment Service Provider at the latest on the first Business Day following the date of receipt of the Payment Order by Credit Transfer. This date of receipt corresponds:

- to the date of validation of the Payment Order by Credit Transfer, for an immediate Credit Transfer;
- to the Execution Date entered, for a scheduled Credit Transfer, provided that the Account to be debited has sufficient and available funds.

We may refuse or defer the execution of a Payment Order by Standard SEPA Credit Transfer transmitted if the mandatory and regulatory information that must appear on the order is incomplete or invalid, or by reason of legal and regulatory obligations — in particular those relating to the fight against money laundering and terrorist financing. In such a situation, unless prohibited by law from doing so, we shall contact you as soon as possible to inform you of the reason for the refusal or deferred execution, and of the possibilities of remedying it.

The Payment Order by Standard SEPA Credit Transfer is processed in batches. We offer you the possibility of withdrawing your consent to execution of the Credit Transfer before the batch is processed. The request to revoke the Payment Order must necessarily arrive before processing of the batch containing the Payment Order.

7.4.4. Execution of International Credit Transfers

Before transmitting a Payment Order by International Credit Transfer, you may view the amount that will be sent in the currency you have chosen, the conversion rate applied and the amount that will be debited from your Account, in addition to the fees applicable in accordance with the Fee Schedule.

Between the time you transmit an international Credit Transfer Order and the time it is executed, the applicable exchange rate may vary. In such case, we automatically adjust the amount that will be debited from your Account, within a 10% limit. If exchange-rate fluctuations would result in your Account being debited by a greater amount, we automatically cancel the International Credit Transfer in order to safeguard your funds.

Subject only to the foregoing, once the Payment Order by International Credit Transfer has been validly transmitted, we credit the account of the Payee's Payment Service Provider on average within 1 to 4 Business Days following receipt of the Payment Order by International Credit Transfer. This date of receipt corresponds to the date of validation of the Payment Order by International Credit Transfer.

However, these time limits are indicative and may vary depending on the time difference, the time at which you issue the Credit Transfer, the currency and the number of correspondent banks that must intervene in the transaction.

We may refuse or defer the execution of a Payment Order by International Credit Transfer transmitted if the mandatory and regulatory information that must appear on the order is incomplete or invalid, or by reason of legal and regulatory obligations — in particular those relating to the fight against money laundering and terrorist financing. In such a situation, unless prohibited by law from doing so, we shall contact you as soon as possible to inform you of the reason for the refusal or deferred execution, and of the possibilities of remedying it.

7.4.5. Execution of TARGET2 Credit Transfers

Access to TARGET2 Credit Transfers is available upon request and subject to our agreement. This type of Credit Transfer is denominated exclusively in euros.

National currencies other than the euro of the Member countries of the SEPA Zone, as well as those of third countries, are not supported.

The maximum amount of a TARGET2 Credit Transfer is set at €50 million.

Once the Payment Order by TARGET2 Credit Transfer has been validly transmitted, we credit the account of the Payee's Payment Service Provider as soon as possible, provided that the request is made between 8 a.m. and 5 p.m. on TARGET2 Business Days.

We may refuse or defer the execution of a Payment Order by TARGET2 Credit Transfer transmitted if the mandatory and regulatory information that must appear on the order is incomplete or invalid, or by reason of legal and regulatory obligations — in particular those relating to the fight against money laundering and terrorist financing.

In such a situation, unless prohibited by law from doing so, we shall contact you as soon as possible to inform you of the reason for the refusal or deferred execution, and of the possibilities of remedying it.

Given the irrevocable nature of TARGET2 Credit Transfers, Payment Orders by TARGET2 Credit Transfer, once executed, may not be the subject of any "recall" or refund request.

7.4.6. Memo Bank Protect

Memo Bank Protect is our anti-fraud feature integrated into the Workspace and the Premium API.

Its purpose is to enhance the security of your Credit Transfers within the SEPA Zone.

The main features of Memo Bank Protect are as follows:

– making available the public legal information (corporate name, SIREN number, etc.) relating to your payees;

- checking the matching of the name and the IBAN as part of Verification of Payee;
- analysis of the fraud history of the IBANs concerned via the databases of payment systems;
- dual validation for the creation of your payees.

You acknowledge and accept that Memo Bank Protect is a decision-support and prevention tool, and not a guarantee against fraud.

The information and alerts we provide to you are based on external data and internal analyses but may not be a substitute for your own vigilance.

You remain solely responsible for the final verification of your payees' details and for authorising your Credit Transfers.

The alerts issued by Memo Bank Protect are not blocking and you may choose not to take them into account. It is for you to take the appropriate measures to assess the risk associated with a Credit Transfer and to decide on its execution.

Accordingly, we disclaim all liability for any loss or damage that you may suffer as a result of fraud if you have decided to override an alert we have issued or to deactivate the Memo Bank Protect features, in particular in the context of a Bulk Credit Transfer.

7.5. Receipt of Payment Orders by Core direct debit debiting an Account

7.5.1. Execution

Officially called "SEPA Direct Debit Core" (SDD Core), the Core direct debit is a means of payment that gives a Payee the possibility of directly debiting funds in euros from the Payer’s account, within the SEPA Zone.

We receive Payment Orders by Core direct debit transmitted by the Payee’s Payment Service Provider at the latest on the Business Day preceding the execution date of the direct debit. The upcoming Core direct debit is then displayed in your Workspace, and you may refuse the Core direct debit at any time until the end of the Business Day preceding the execution date. We execute the Payment Order by Core direct debit received on the execution date provided that:

- at the time we execute the order, your Account has sufficient and available funds;
- the Payment Order by Core direct debit transmitted by the Payee’s Payment Service Provider is complete and consistent.

The Payment Order by Core direct debit contains a mandate by which:

- you authorise the Payee to transmit to us Payment Orders by Core direct debit to debit your Account;
- you authorise us to debit your Account, in execution of Payment Orders by Core direct debit received from your Payee.

From the receipt of an initial Payment Order by Core direct debit issued by a given Payee, the associated Core Direct Debit Mandate will appear in your Workspace in the list of "Active Mandates".

We are under no obligation to check the data of the Core Direct Debit Mandate contained in the Payment Order by Core direct debit. We may reject the execution of a Payment Order by Core direct debit transmitted if the above conditions are not met, or by reason of legal and regulatory obligations

— in particular those relating to the fight against money laundering and terrorist financing. In such a situation, unless prohibited by law from doing so, we shall contact you as soon as possible to inform you of the reason for the refusal or deferred execution, and of the possibilities of remedying it.

7.5.2. Suspension and cancellation of the mandate

You may at any time suspend an active Core Direct Debit Mandate directly in your Workspace; all future Payment Orders by Core direct debit linked to the Core Direct Debit Mandate in question will then be rejected. To avoid any dispute with the Payee, we recommend that you inform them beforehand.

It is your responsibility, if you wish to suspend or cancel a Core Direct Debit Mandate, to suspend or cancel that mandate directly in your Workspace. No other means of suspending a Core Direct Debit Mandate may be accepted. In any event, we are not liable for the consequences arising from a Core Direct Debit Mandate that has not been updated in your Workspace.

7.5.3. Lapse of the mandate

A Core Direct Debit Mandate in respect of which no new Payment Order by Core direct debit has been presented for 36 months lapses and may no longer be used.

7.6. Receipt of Payment Orders by B2B direct debit debiting an Account

7.6.1. Consent

Officially called "SEPA Direct Debit B2B" (SDD B2B), the B2B direct debit is a means of payment similar to the Core direct debit, but with limited refund conditions (the dispute conditions are listed in clause 7.8, “Dispute of a Payment Transaction”). For this reason, it is used only to manage the collection of payments between businesses. It does not apply to consumers or to sole traders. We therefore require, for its execution, that the User comply with the following B2B mandate validation procedure:

– before the one-off B2B direct debit (or before the first B2B direct debit, if recurring), access the "direct debits" tab of your Workspace then click on "New B2B mandate";

– follow the instructions, sending us a copy of the valid B2B Direct Debit Mandate — it must in particular be signed by a duly empowered natural person;

– confirm by entering the form data (Payee’s name, ICS number and mandate reference) using the information present on the B2B Direct Debit Mandate attached at the previous step;

– we then verify that the B2B Direct Debit Mandate transmitted is valid and that it corresponds to the data entered in the form.

This B2B Direct Debit Mandate validation procedure is the only one we accept. Its application by the User constitutes your consent to the execution of future Payment Orders by B2B direct debit linked to the mandate in question.

Once this B2B Direct Debit Mandate validation procedure has been completed, the B2B Direct Debit Mandate will appear in your Workspace in the list of "active mandates".

7.6.2. Execution

We receive Payment Orders by B2B direct debit transmitted by the Payee's Payment Service Provider at the latest on the Business Day preceding the execution date of the order. The upcoming B2B direct debit is then displayed in your Workspace and you may, where applicable, refuse the Payment Order by B2B direct debit until 10:00 a.m. (Paris time, France) on the Business Day preceding the execution date.

We execute the Payment Order by B2B direct debit received (as well as any subsequent Payment Order by B2B direct debit, in the case of recurring direct debits) on the execution date defined, subject to the following conditions:

- at the time we execute the order, your Account has sufficient and available funds;
- a B2B Direct Debit Mandate has been validly added to the list of your mandates, after carrying out the B2B mandate validation procedure described in clause 7.6.1, "Consent";
- the Payment Order by B2B direct debit transmitted by the Payee's Payment Service Provider is complete and consistent with the data of the form entered during the B2B mandate validation procedure.

We may reject the execution of a Payment Order by B2B direct debit transmitted if the above conditions are not met, or by reason of legal and regulatory obligations — in particular those relating to the fight against money laundering and terrorist financing. In such a situation, unless prohibited by law from doing so, we shall contact you as soon as possible to inform you of the reason for the refusal or deferred execution, and of the possibilities of remedying it.

7.6.3. Suspension or cancellation of the mandate

You may at any time suspend a B2B Direct Debit Mandate directly in your Workspace; all future Payment Orders by B2B direct debit linked to the B2B Direct Debit Mandate in question will then be rejected.

It is your responsibility, if you wish to suspend or cancel a B2B Direct Debit Mandate, to suspend or cancel that mandate directly in your Workspace. No other means of suspending a B2B Direct Debit Mandate may be accepted. Consequently, we are not liable for the consequences arising from a B2B Direct Debit Mandate that has not been updated in your Workspace.

7.6.4. Lapse of the mandate

A B2B Direct Debit Mandate in respect of which no new Payment Order by B2B direct debit has been presented for 36 months lapses and may no longer be used. In that case, you will need to enter and validate a new B2B Direct Debit Mandate via the B2B mandate validation procedure described in clause 7.6.1, "Consent".

7.7. Processing and foreign exchange of Payment Transactions in foreign currencies

When you receive a Payment Order by Credit Transfer in foreign currency, its processing depends on the Account that is the recipient of the payment:

- if you hold an Account denominated in that currency, the Payment Transaction is credited directly to it, without conversion;

– if you do not hold an Account in that currency, the Payment Transaction is converted into the currency of the relevant Account; the conversion is carried out at the reference exchange rate in force on the day of processing, and the fees set out in our Fee Schedule apply;

– if the currency is not eligible, the Payment Transaction is rejected.

If a Payment Transaction in foreign currency is cancelled after having been credited in euros to your Account, you bear the resulting foreign-exchange risk, whether it translates into a gain or a loss.

7.8. Dispute of a Payment Transaction

Generally speaking, in the event of a dispute, we will do our utmost to help you — and, where appropriate, refund you. You will find below the conditions and arrangements applicable to disputes of Payment Transactions, depending on whether the relevant Payment Transaction was authorised (or not) and correctly executed (or not). Any dispute of a Payment Transaction may give rise to the fees set out in the Fee Schedule being charged.

In this respect, if you consider that a Payment Transaction is unauthorised or defectively executed, it is for you, by way of derogation from Article L. 133-23 of the French Monetary and Financial Code, to provide evidence thereof.

7.8.1. Dispute of an authorised transaction

	Correctly executed transaction	**Defectively executed transaction**
SEPA Credit Transfer issued	No right to a refund if you dispute the transaction, but we will do our utmost to recover your money from the Payee.	Right to a refund if you dispute the transaction before the expiry of a maximum 8-week period from the date on which the funds were debited (by way of derogation from Article L. 133-24, first paragraph, of the French Monetary and Financial Code).
Core direct debit	Right to a refund if you dispute the transaction before the expiry of a maximum 8-week period from the date on which the funds were debited.	Right to a refund if you dispute the transaction before the expiry of an 8-week period from the date on which the funds were debited (by way of derogation from Article L. 133-24, first paragraph, of the French Monetary and Financial Code).

	Correctly executed transaction	Defectively executed transaction
B2B direct debit	No right to a refund if you dispute the transaction (by way of derogation from Article L. 133-25-1 of the French Monetary and Financial Code, you waive your right to request a refund of the transaction).	Right to a refund if you dispute the transaction before the expiry of a period of 2 Working Days from the date on which the funds were debited (by way of derogation from Articles L. 133-24, first paragraph, and L. 133-25-1 of the French Monetary and Financial Code).

7.8.2. Dispute of an unauthorised transaction

<table>
<tr><th></th><th>Loss or theft of Personalised Security Credentials</th><th>Other cases</th></tr>
<tr><td>SEPA Credit Transfer issued</td><td rowspan="2">No right to a refund for any loss suffered before notification of the loss or theft for the purposes of blocking (by way of derogation from Article L. 133-19, I). Right to a refund for any loss suffered after notification of the loss or theft for the purposes of blocking, in accordance with the arrangements described in clause 5.12, “Personalised Security Credentials”, up to a limit of €2,500, save for fraudulent conduct on your part or if you have not, intentionally or through gross negligence, complied with the obligations set out in Articles L. 133-16 and L. 133-17 of the French Monetary and Financial Code (by way of derogation from Article L. 133-20).</td><td>Right to a refund if you dispute the transaction before the expiry of a maximum 8-week period from the date on which the funds were debited (by way of derogation from Article L. 133-24, first paragraph, of the French Monetary and Financial Code), unless we suspect fraud on your part. In the latter case, we shall inform the Banque de France.</td></tr>
<tr><td>Core direct debit</td><td>Right to a refund if you dispute the transaction before the expiry of an 8-week period from the date on which the funds were debited (by way of derogation from Article L. 133-24, first paragraph, of the French Monetary and Financial Code), unless we suspect fraud on your part. In the latter case, we shall inform the Banque de France.</td></tr>
</table>

	Loss or theft of Personalised Security Credentials	Other cases
B2B direct debit		Right to a refund if you dispute the transaction before the expiry of a period of 2 Working Days from the date on which the funds were debited (by way of derogation from Articles L. 133-24, first paragraph, and L. 133-25-1 of the French Monetary and Financial Code), unless we suspect fraud on your part. In the latter case, we shall inform the Banque de France.

8. EBICS

We offer only the EBICS-TS protocol. Only the versions of EBICS-TS indicated in our online help are handled by our system.

The use of EBICS implies that you have specific software, an EBICS client, allowing communication with our systems.

8.1. Activation of the EBICS connection

You may create an EBICS connection for each User of your Workspace. Any new creation of an EBICS connection will generate new credentials in your Workspace. These credentials, necessary for configuring your EBICS client, will be made available to the Representative and the authorised Users of your Workspace.

To configure your EBICS client, you will need to provide it with certificates issued by a recognised certification authority.

To finalise the activation of your EBICS connection, you will need to send us, via your Workspace, the initialisation letters generated by your EBICS client.

Each User will finally need to validate their EBICS connection by means of Strong Customer Authentication.

The EBICS connection will be invoiced to you from the first active User in accordance with our Fee Schedule.

8.2. Downloading of account statements

Once your EBICS connection is active, account statements will be made available on your EBICS client. The frequency at which these account statements are made available will depend on the configuration of your EBICS client.

8.3. Issuance of Payment Orders by SEPA Credit Transfer

Users authorised to execute Payment Orders by SEPA Credit Transfer from their Workspace may issue and sign Payment Orders by SEPA Credit Transfer from their EBICS client. These Payment Orders by SEPA Credit Transfer will be processed in accordance with the information indicated in the SEPA Credit Transfer files. The execution of the Payment Orders by SEPA Credit Transfer will proceed in accordance with the Payment Orders by SEPA Credit Transfer entered directly from your Workspace.

8.4. Closure of an EBICS connection

You may at any time close one or more EBICS connections in your Workspace. A closed EBICS connection cannot be recovered and a new EBICS connection will need to be created. The invoicing of the EBICS service will end on the closure of the last active EBICS connection.

9. Enforcement measures brought by third parties

Your creditors, holding an enforceable title or judicial authorisation, may take enforcement measures against you, such as protective attachments, garnishments or, in the case of the administration, administrative seizures in the hands of a third party.

In accordance with the law, such attachments may render unavailable the balance of your Accounts as well as your Term Deposit Accounts from the day on which they are served on or notified to us.

If the balance of your Accounts denominated in the currency of the enforcement measure is not sufficient to satisfy the attaching creditor, the balance of your other Accounts is converted into that currency at the reference exchange rate in force on the day of payment.

10. Liability

We undertake to provide you with the best possible Services, under a best-efforts obligation.

We shall not be liable if the Services come to be interrupted, suspended, degraded or rendered temporarily inaccessible, suffer a technical difficulty (sending, receipt, processing or transmission of data), or are affected by an overload, malfunction, cyberattack, force majeure event or any event beyond our reasonable control (including disruptions to the Internet network, hosting infrastructures or telecommunications networks). This limitation applies whether the interruption is total or partial, one-off or recurring.

We also disclaim all liability for any direct or indirect damage resulting from the use of information that has not been updated by you in accordance with clause 6, "Communication and updating of your data", including where the inaccuracy or obsolescence of such information is the cause of a refusal, delay or error of execution.

Likewise, we shall not be liable for any direct, indirect or consequential damage resulting from the implementation of legal and regulatory obligations incumbent upon us (for example: an asset-freezing measure, the blocking or suspension of a Transaction for reasons related to the fight against money laundering and terrorist financing, or the implementation of Verification of Payee), in particular in the event of delays, rejections or non-execution of Payment Transactions, even where such measures cause you financial or commercial harm.

We shall not be liable in the event of total or partial impossibility of executing a foreign-exchange or payment transaction in foreign currency due to exceptional instability of the financial markets, unavailability or suspension of the applicable reference rates, or any regulatory restriction or decision of a competent authority affecting the foreign-exchange markets.

We shall not be liable for any damage resulting from a technical failure, interruption or malfunction of the Verification of Payee service, the inaccuracy, incompleteness or out-of-date nature of the data provided by third-party Payment Service Providers for that service, or where you decide to proceed with a Credit Transfer notwithstanding our prior notification of any mismatch, of whatever nature, between the name and the IBAN of a Payee. In the latter case, you alone and entirely bear the consequences of your decision to override our warning.

You are also exclusively and irrevocably liable for the contents you upload to the Workspace (such as invoices, receipts, statements or any other document), of which we cannot guarantee the accuracy, integrity, authenticity or evidential force. You remain the sole judge of the relevance and reliability of the documents you choose to import.

Nor shall we be liable for any error, omission or inaccuracy in the data you may extract, manually or by any automated process, from such content, or for any accounting, tax or financial errors found after using the tools made available to you under the Services.

11. Evidence agreement

You acknowledge and accept that the electronic signature method used to enter into the Agreement is enforceable against you, evidences your consent to the rights and obligations arising from the Agreement and produces legal effects in the same way as a handwritten signature. The Agreement signed in electronic form therefore has the status of an original document with evidential force.

You acknowledge and accept that the method for granting a Power of Attorney described in clause 5.10, “Users — Power of Attorney” is enforceable against you, evidences your consent to the rights and obligations arising from the grant of a Power of Attorney and produces legal effects in the same way as a handwritten signature.

You acknowledge and accept that we may send you all correspondence by electronic means and in particular by email. You shall be deemed to have indisputably been made aware of messages, information and attachments by the sole fact of their dispatch to the email address registered in the Workspace.

In addition, you acknowledge and accept that all forms of recording resulting from the means of communication used — in particular IT records (email, any action carried out by a duly authenticated User in the Workspace), as well as timestamps in our IT systems — are admissible as evidence. Any confirmation of action on your part via the Simple Authentication or Strong Customer Authentication procedures constitutes your agreement.

In particular, as regards the rules of admissible evidence in connection with the performance of our Services, you acknowledge and accept:

- that the evidence of Payment Orders transmitted after Simple Authentication or Strong Customer Authentication may be provided by the reproduction on IT medium of the authentication elements that we record, and that shall be authentic. We may certify Execution Dates of Payment Transactions on the Account by a timestamping process. This process shall constitute evidence of the data it contains;
- the recording of all electronic communications between us and you for the purposes of evidence and improvement of the Services;

- the recording of telephone conversations, in particular for the purposes of follow-up, security and evidence (for example, to verify proper understanding of your instructions through a callback) and the improvement of our Services.

12. Single account

Save for express derogation, all Accounts opened in your name, whether in credit or in debit, form the parts of a single and indivisible account, even if they are separate and bear different identification numbers. In the event of closure of our business relationship, the balance due corresponds to the balance of that single and indivisible account.

To calculate it, the balance of your Foreign Currency Accounts is converted into euros at the reference exchange rate in force on the day of calculation, with application of the foreign-exchange fees provided for in the Fee Schedule.

This rule does not prevent each of your Accounts from generating interest, whether debit or credit.

13. Deposit guarantee

Your deposits, including your foreign-currency deposits, are covered by a guarantee scheme managed by the Deposit Guarantee and Resolution Fund (FGDR), which compensates you up to €100,000, regardless of the number of Accounts opened with us. These are exactly the same conditions as in all other banks. To find out more, you can:

- read the Schedule I, *General information on the protection of deposits*;
- read our online help;
- consult the website of the Deposit Guarantee and Resolution Fund.

14. Professional secrecy

Like any bank, we are bound by professional secrecy. We may, however, be required to transmit data covered by professional secrecy to certain service providers to whom we delegate tasks in strict compliance with the law.

You may at any time authorise us to waive professional secrecy vis-à-vis a third party by notifying us in writing — this is the case, for example, when you sign the Power of Attorney when adding a new User, or when you use an Account Information Service Provider or a Payment Initiation Service Provider. The third party who receives the information covered by professional secrecy shall in turn be bound to keep it strictly confidential.

15. Personal data

We may collect personal data concerning you (and more particularly the legal representatives, beneficial owners and Users).

We invite you in this respect to consult the Memo Bank Personal Data Protection Policy, which describes the purposes of the processing of the personal data collected, the arrangements for its communication to third parties, your rights relating to such data and the security measures put in place.

16. Right of withdrawal

Where the Agreement has been entered into in the context of a Banking Solicitation operation, you have a period of 14 days from its signature to exercise your right of withdrawal by sending us an email to retractation-compte@memo.bank. You are then required to return to us any outstanding debts (in particular the balance of your Accounts if they are in debit), while we are required to return to you the balance of your Accounts, if they are in credit. Any sum you owe us shall bear interest at the interest rate set out in the Fee Schedule until full payment, as provided for the closure of your Accounts in clause 19, "Termination".

17. Set-off

You expressly authorise us to set off, at any time and without prior formality, any claim we hold against you, whether certain, liquid and payable or not, against the credit balance of any of your Accounts.

This authorisation extends to related claims arising from separate transactions as well as to future or conditional claims, provided that they have their origin in the Agreement or in any other contractual relationship between us.

Set-off may be carried out at any time, and in particular upon closure of one of your Accounts or termination of the Agreement. Where applicable, the balance of your Foreign Currency Accounts shall be converted into euros at the reference exchange rate in force on the day of set-off.

18. Complaints

If you have a complaint, you may contact our customer-service team by email at: contact@memo.bank.

19. Termination

The Agreement may be terminated at any time, by you or by us, subject to 30 days' notice, without need for cause.

If you have subscribed to a subscription with a Commitment:

- termination of the services agreement before the expiry of the Commitment shall not give rise to any refund of sums already paid, even if these exceed your actual Usage;
- you remain liable for the portion of the Commitment corresponding to the number of days elapsed since the start of the Period, or for your actual Usage if the latter is higher.

By way of exception, this portion of the Commitment is not due if termination follows your refusal of an amendment to the Agreement that we have decided.

In all cases, if termination is at our initiative, we will inform you by email. If you wish to terminate, you need only send us your request by email to resiliation-compte@memo.bank.

The Agreement shall be terminated by operation of law and without prior formal notice in the following cases:

- failure to comply with the provisions of the Agreement;
- abnormal operation of an Account;
- serious misconduct on your part. For example: illegal activities, fraudulent conduct or false declarations;
- loss, withdrawal, suspension or non-renewal of an authorisation, approval, licence, registration in a professional register, financial guarantee, regulated surety or any other compulsory insurance required for the conduct of your activity.

Termination of the Agreement entails the closure of your Accounts.

On closure of your Accounts, you undertake:

- in the event of a credit balance on your Accounts, to indicate to us the identifier of the bank account to which the balance of your Accounts is to be transferred, by Credit Transfer; if this account is not denominated in the same currency as the Account being closed, we shall carry out a conversion into euros (or into the destination currency) at the reference exchange rate in force on the day of the credit transfer, with application of the foreign-exchange fees set out in our Fee Schedule; the amount transferred is established net of any sum that may be due to us;
- in the event of a debit balance on your Accounts, to settle any debit balance existing on the day of closure, it being specified that interest shall accrue on this debit balance at the rate applied to unauthorised overdrafts on the day of closure, in accordance with our Fee Schedule in force; pursuant to Article 1343-2 of the French Civil Code, interest due for a whole year will itself bear interest; it is payable at any time and until full payment; in the event of a debit balance on a Foreign Currency Account, the latter may be converted into euros at the reference exchange rate in force on the day of closure, with application of the foreign-exchange fees set out in our Fee Schedule.

20. Governing law

The applicable law is French law. Any dispute relating to this Agreement shall fall, failing amicable resolution, within the jurisdiction of the courts within the jurisdiction of the Paris Court of Appeal, including in the event of multiple defendants, third-party proceedings or protective proceedings.

Schedule A: Terms of use of Visa cards

A.1. Presentation of the Visa card

The Card is a means of payment that must be used exclusively for professional purposes.

The Virtual Card and the Physical Card allow you to settle purchases of goods and services on your behalf with service providers and merchants belonging to the Visa network and equipped with a compatible electronic payment terminal (whether contact or contactless), or remotely, in particular by telephone or over the Internet.

The Physical Card allows cash or foreign-currency withdrawals to be made in France and abroad from ATMs approved by the Visa network.

A.2. Ordering Cards

The Representative may, through the Workspace, order and activate one or more Physical Cards, as well as one or more Virtual Cards, which shall be strictly personal to them and may not be used by a third party.

They may also grant a Power of Attorney to one or more Users to order one or more Physical Cards, as well as one or more Virtual Cards.

For obvious security reasons, the Representative shall grant a Power of Attorney only to Users who are authorised to make payments in your name and on your behalf.

Any person who holds a Card, whether the Representative or a User, is designated as a Cardholder.

In order to use a Card, the Cardholder undertakes to provide all the information that we may request, in particular for regulatory reasons.

Physical Cards are sent by post to the address specified at the time of their order.

The Cardholder must sign their Physical Card in the space provided for that purpose, as soon as they receive it.

Virtual Cards ordered are made available in the Workspace.

A.3. Fee Schedule

The obtaining of Cards and their use may give rise to the fees set out in the Fee Schedule being charged.

These fees are debited from your Principal Account.

A.4. Maximum amount of Card payments and debits

Payments made by Card are subject to deferred debiting within the limit of an overall maximum amount that we set for the Representative and the Users of your Accounts.

All deferred-debit Card payments made during a calendar month within the limit of this amount are thus subject to a single debit on a date indicated in the Workspace.

The overall maximum amount of deferred-debit Card payments is also indicated in the Workspace. Any request to amend it shall be subject to our agreement.

Payments made above this amount are automatically subject to instant debiting.

If you do not wish Card payments to be subject to deferred debiting for a particular Card, you may deactivate this feature for that Card in the Workspace. Payments made with that Card will then be debited instantly. You may reactivate deferred debiting for that Card at any time.

The Representative has the option of setting a maximum amount of payments over a given period for each Card.

Cash withdrawals are always debited instantly.

You must ensure that, on the day of debiting of settlements made using your Cards, each of your Accounts has a sufficient available balance.

A.5. Consent of the Cardholder to make a payment

When a Cardholder gives a Payment Order using their Card, we consider that their agreement is firm and irrevocable as soon as they:

- enter their PIN code on an ATM or electronic payment terminal;
- insert their Card into an electronic device without a keypad for entering a code (for example, a motorway toll);
- communicate and confirm the data relating to the remote use of their Card, equivalent to Strong Customer Authentication of the Cardholder;
- present their Card to a contactless payment device;
- sign by hand a ticket issued by the electronic device for both the Acquirer and the Cardholder.

A.6. Execution of a Payment Order

We receive a Payment Order by Card at the time it is communicated to us by the Acquirer’s payment service provider.

Where the Payment Order by Card is executed within the European Economic Area, the amount of the payment transaction is credited to the account of the Payee’s Payment Service Provider at the latest at the end of the following Business Day.

We may refuse or defer the execution of a Payment Order by Card transmitted if the mandatory and regulatory information that must appear on the Order is incomplete or invalid, or by reason of legal and regulatory obligations — in particular those relating to the fight against money laundering and terrorist financing. In such a situation, unless prohibited by law from doing so, we shall contact you as soon as possible to inform you of the reason for the refusal or deferred execution, and of the possibilities of remedying it.

A.7. Security measures relating to the use of the Card

A.7.1. Measures specific to the Physical Card

A personal PIN code is made available to the Cardholder in their Workspace. This code is requested when making a payment via an electronic payment terminal or making a cash withdrawal.

The PIN code may be entered up to three consecutive attempts. If the Cardholder enters an incorrect code three times, the Card may no longer be used for any payment requiring entry of the PIN code, including for a cash withdrawal. In the latter case, the Card is also liable to be captured by the ATM.

In such situation, it is for the Cardholder to request the sending of a new Card from their Workspace.

The Cardholder must take all necessary measures to ensure the security of their Card and of the PIN code. In particular, the Cardholder must not communicate it to a third party, nor write it on a paper document or a digital medium that is not secured by Strong Customer Authentication. The Cardholder must never communicate their PIN code, for any reason, including to their bank or to other Users of their Workspace.

A.7.2. Measures specific to contactless payment by Physical Card

Contactless payment requires the presence of a pictogram on the Acquirer's electronic payment terminal indicating that such payment method is possible.

Contactless payment is limited to an amount defined by the regulations or by Visa. For your information, it is currently set at €50.

When this limit is reached, the next payment made with your Physical Card will require you to enter your PIN code.

A.7.3. Measures specific to remote payment by Card

The Cardholder may make a payment by Card remotely, whether over the Internet or by telephone.

In such case, they will be asked to communicate the Card number, the expiry date and the visual cryptogram appearing on the Virtual Card or on the back of the Physical Card. During the remote payment process, we may ask the Cardholder to validate the payment by Strong Customer Authentication, via the mobile application.

A.8. Use of the Card from or to abroad, and exchange rate

Where a Cardholder makes a payment with a Card to an Acquirer located outside the euro area, the conversion into euros is carried out by Visa on the day the payment transaction is processed in accordance with its exchange conditions in force on that date. In addition, we charge a commission in accordance with the Fee Schedule in force at the time of the payment.

A.9. Liability and obligations of the Cardholder

The Cardholder must systematically:

- ensure that the payments they make with the Card are made in the course of their professional activity;
- ensure that the payments or cash withdrawals made with their Card are made to merchants, service providers or ATMs approved by Visa and bearing a Visa logo;
- observe the security measures specific to the use of their Card, in particular by not communicating their PIN code and by complying with the authentication procedures we put in place;
- not make any modification, marking or alteration to their Card;
- block their Card from their Workspace as soon as possible in the event of loss, theft or suspicion of fraudulent use; any other means may result in delays in handling the request;
- make no false declaration, on pain of incurring civil and criminal liability;
- destroy their Physical Card without delay once it has expired.

A.10. Our liability in the event of an unauthorised or defectively executed payment

If a Cardholder finds that a Payment Transaction debiting your Account was not authorised or that there has been an error in the processing of a Payment Order by Card, it is necessary, after having blocked the Card from their Workspace, to report it to us as soon as possible by email or by telephone.

In any event, it is essential to send us by email all useful supporting documents (such as a copy of a police complaint) within a maximum of 8 weeks from the date the disputed Payment Order was debited from the Account.

This period is reduced to seventy days if the Payee's Payment Service Provider is located in a State that is neither a Member State of the European Union nor a Member State of the European Economic Area.

If it is established that a Payment Transaction was not authorised or in the event of failure on our part in respect of a defectively executed payment transaction, we will return the corresponding amount to you and restore your Account to the situation that would have prevailed had the defective Payment Transaction not taken place.

However, we will not be able to refund you:

- in the event of fraud or negligence on the part of the Cardholder;
- unauthorised Card payments that were made before the Card was blocked in the event of loss or theft of the Card or of the Personalised Security Credentials; these will then be borne by you; unauthorised Card payments made after the Card was blocked are refunded up to a limit of €2,500;
- if, in your view, the payment transaction by Card has been defectively executed whereas we have found that it has been duly carried out, correctly authenticated, recorded and accounted for without technical failure;
- if the Payment Transaction by Card was defectively executed because of a delay whereas we did transfer the funds to the Payee within the time limits provided for by the regulations and these Terms of Use;
- if the Payment Transaction by Card was defectively executed or could not be executed because the Cardholder communicated an inaccurate Card number, an incorrect expiry date or an erroneous cryptogram;
- where legal or regulatory obligations do not allow us to execute the Payment Transaction by Card;
- in the event of force majeure.

In accordance with the Fee Schedule, fees may be charged in the event of an unjustified dispute of a Payment Transaction by Card.

Finally, we shall not be liable for an Acquirer's refusal to accept a Card payment or for any commercial dispute, nor guarantee the proper functioning of an Acquirer's electronic payment terminal or the availability of cash in an ATM.

A.11. Information communicated on the Workspace and account statements

In accordance with the regulations, immediately after receiving the Payment Order, we make available to you, on your Workspace:

- the references enabling you to identify the payment transaction by Card and, where applicable, the information relating to the Payee;
- the amount of the payment transaction by Card expressed in the currency used in the Payment Order;
- the amount of any fees attributable to you and, where applicable, the breakdown of these fees;

- where applicable, the reference exchange rate applied to the payment transaction by Card and the amount of the transaction after such currency conversion; the exchange rate applicable on the day of processing of the transaction is indicated on your account statement;
- the date of receipt of the Payment Order by Card.

A.12. Period of validity of the Card

The expiry date of Physical Cards is shown on the back of each Card. Once the validity date has passed, it is your responsibility to destroy the Physical Card.

They are automatically renewed and sent to the address registered in the Workspace.

As regards Virtual Cards, their period of validity is set out in the Workspace. They are automatically renewed upon expiry, unless you have decided to use a single-use Virtual Card.

A.13. Suspension of the service and termination

These Terms of Use may be terminated at our initiative at any time, by email, subject to 30 days' notice, without need for cause.
We may also terminate the Terms of Use or suspend their performance without observing any notice period in the following cases:

- failure to comply with the Terms of Use;
- abnormal operation of an Account;
- abusive or seriously reprehensible conduct on your part. By way of example, this includes the following situations:
  - the provision or delivery of documents that prove to be inaccurate, false or falsified;
  - in the event of insufficient available balance, despite our reminders and warnings;
  - a criminal conviction (other than for a minor offence);
- where your situation proves to be irremediably compromised.

If you wish to permanently stop using one or more Cards, you need only go to your Workspace to delete them. In the case of paid Cards that you have ordered, they will no longer be invoiced as from such deletion.

A.14. Protection of personal data

We may collect personal data concerning you as well as the Representative or the Cardholders, namely the data recorded or generated by means of the Card and those relating to payments made with the Card.

We invite you in this respect to consult the Memo Bank Personal Data Protection Policy, which describes the purposes of the processing of the personal data collected, the arrangements for its communication to third parties, your rights relating to such data and the security measures put in place.

Schedule B: Terms of use of Apple Pay

B.1. Presentation of Apple Pay

Apple Pay is a service developed by Apple Inc. that allows you to use your Virtual Cards and to dematerialise and use your Physical Cards to make payments, in person or remotely, using a compatible Apple device, namely an iPhone (with Face ID or Touch ID, except the iPhone 5s, or a later version), an iPad (with Touch ID or Face ID, or a later version), an Apple Watch or a Mac (models on sale since 2012), it being noted that this list may evolve.

Apple Pay uses a technology called "tokenisation" to protect the information of the Cardholders' Cards. This technology replaces the Card information with a unique number for each transaction.

Payment Transactions carried out using Apple Pay are considered to be Payment Transactions by Card and are therefore subject to the same rules, in particular as regards the liability of the Cardholder and the arrangements for deferred or instant debiting of your Account.

B.2. Activation of Apple Pay

To use Apple Pay with a Physical or Virtual Card, that Card must already have been activated in the Workspace.

Furthermore, the Cardholder must have an iCloud account.

To register a Card in Apple Pay, the Cardholder may use:

- Memo Bank's mobile application, which requires iOS 14 or a later version;
- the "Wallet" app that appears by default on iPhones and iPads;
- "Settings" on iOS or "System Settings" on macOS;
- the "Watch" app on an iPhone.

They will then have to enter the Card details required for registration or use the camera of their Apple device to scan that same information.

After confirming this information by Strong Customer Authentication, the Cardholder is then invited to accept these terms of use and Memo Bank's privacy policy.

B.3. Consent of the Cardholder to make a payment

When a Cardholder gives a Payment Order using Apple Pay, we consider that their agreement is firm and irrevocable as soon as:

- in order to make a remote payment, they use one of the authentication methods provided by Apple; depending on the device used, this may be Touch ID, Face ID, an unlock code or the use of the Apple Watch paired with an iPhone;
- in order to make a payment to a merchant or a service provider, they present their Apple device to a compatible contactless payment device.

We draw your attention to the fact that the use of Apple Pay with a contactless payment device is not limited to €50 as for a Physical Card. The contactless payment limit is the one imposed by the Acquirer's payment terminal.

B.4. Security measures relating to the use of Apple Pay

The Cardholder must take all necessary measures to ensure the security of their Apple device and, in particular, of their unlock code, which they must neither communicate to a third party nor write on a paper document or digital medium not secured by Strong Customer Authentication. The Cardholder must never communicate their unlock code, for any reason, including to us or to other Users of their Workspace.

Likewise, the Cardholder must not allow anyone to register biometric information allowing the use of Touch ID or Face ID on their Apple device after registering a Card in Apple Pay.

Indeed, any person knowing the Cardholder's unlock code or whose biometric information is registered in the Cardholder's Apple device will be able to make payments with a Card registered in Apple Pay. Such payments will be valid, authorised and therefore irrevocable, exempting us from any liability in the event of an abusive or fraudulent Payment Transaction.

We remind you that the rules on unauthorised or defectively executed Card payments apply fully to Payment Transactions carried out using Apple Pay.

B.5. Suspension and blocking of Apple Pay by the Cardholder

The Cardholder has the possibility of temporarily suspending or removing a Card registered in Apple Pay, including remotely, using their iCloud account.

However, in such case, Payment Transactions pending processing will be settled normally and the Card may still be used independently of Apple Pay.

Therefore, where a Cardholder finds that a Payment Transaction carried out using Apple Pay was not authorised or that there has been an error in the processing of a Payment Order, it remains necessary to block the relevant Card in the Workspace and to report it to us as soon as possible by email or by telephone.

B.6. Suspension and blocking of Apple Pay by Apple

We shall not be liable for any blocking of the use of Apple Pay due to a malfunction of the device or of an Apple application of the Cardholder, or a decision by Apple to suspend or block its services for any reason whatsoever, in particular for technical reasons or use that does not comply with Apple's terms of use.

B.7. Intellectual property

Apple, Apple Pay, Face ID, Touch ID, Apple Watch, Mac, macOS, iOS, iPad and iPhone are trademarks of Apple Inc., registered in the United States and other countries.

Schedule C: Terms of use of Google Pay

C.1. Presentation of Google Pay

Google Pay is a service developed by Google that allows you to use your Virtual Cards and to dematerialise and use your Physical Cards to make payments, in person or remotely, using an Internet browser or a compatible Android device, namely a smartphone or tablet equipped with an NFC (Near Field Communication) chip and on which Android 7.0 or a later version is installed, it being noted that this list may evolve.

Google Pay uses a technology called "tokenisation" to protect the information of the Cardholders' Cards. This technology replaces the Card information with a unique number for each transaction.

Payment Transactions carried out using Google Pay are considered to be Payment Transactions by Card and are therefore subject to the same rules, in particular as regards the liability of the Cardholder and the arrangements for deferred or instant debiting of your Account.

C.2. Activation of Google Pay

To use Google Pay with a Physical or Virtual Card, that Card must already have been activated in the Workspace.

Furthermore, the Cardholder must have a Google account.

To register a Card in Google Pay, the Cardholder may use:

- Memo Bank's mobile application;
- the Google Wallet app, which is available on the Google Play Store;
- the Google Play Store app;
- a Google Chrome browser by going to the settings page;
- another Internet browser by going to the website pay.google.com.

They will then have to enter the Card details required for registration or use the camera of their Android device to scan that same information.

After confirming this information by Strong Customer Authentication, the Cardholder is then invited to accept these terms of use and Memo Bank's privacy policy.

C.3. Consent of the Cardholder to make a payment

When a Cardholder gives a Payment Order using Google Pay, we consider that their agreement is firm and irrevocable as soon as:

- in order to make a remote payment, they use one of the authentication methods provided by Google; depending on the device used, this may be an unlock code or biometric identification by fingerprint or facial recognition;
- in order to make a payment to a merchant or a service provider, they present their Android device to a compatible contactless payment device.

We draw your attention to the fact that the use of Google Pay with a contactless payment device is not limited to €50 as for a Physical Card. The contactless payment limit is the one imposed by the Acquirer's payment terminal.

C.4. Security measures relating to the use of Google Pay

The Cardholder must take all necessary measures to ensure the security of their Android device and, in particular, of their unlock code, which they must neither communicate to a third party nor write on a paper document or digital medium not secured by Strong Customer Authentication. The Cardholder must never communicate their unlock code, for any reason, including to us or to other Users of their Workspace.

Likewise, the Cardholder must not allow anyone to register biometric information allowing their Android device to be unlocked after registering a Card in Google Pay.

Indeed, any person knowing the Cardholder's unlock code or whose biometric information is registered in the Cardholder's Android device will be able to make payments with a Card registered in Google Pay. Such payments will be valid, authorised and therefore irrevocable, exempting us from any liability in the event of an abusive or fraudulent Payment Transaction.

We remind you that the rules on unauthorised or defectively executed Card payments apply fully to Payment Transactions carried out using Google Pay.

C.5. Suspension and blocking of Google Pay by the Cardholder

The Cardholder has the possibility of temporarily suspending or removing a Card registered in Google Pay, including remotely, using their Google account.

However, in such case, Payment Transactions pending processing will be settled normally and the Card may still be used independently of Google Pay.

Therefore, where a Cardholder finds that a Payment Transaction carried out using Google Pay was not authorised or that there has been an error in the processing of a Payment Order, it remains necessary to block the relevant Card in the Workspace and to report it to us as soon as possible by email or by telephone.

C.6. Suspension and blocking of Google Pay by Google

We shall not be liable for any blocking of the use of Google Pay due to a malfunction of the device or of a Google application of the Cardholder, or a decision by Google to suspend or block its services for any reason whatsoever, in particular for technical reasons or use that does not comply with Google's terms of use.

C.7. Intellectual property

Google, Google Pay, Google Play and Android are trademarks of Google LLC, registered in the United States and other countries.

Schedule D: General terms and conditions of investment services

D.1. Preamble

These general terms and conditions of investment services (hereinafter the "IS Terms") are intended to govern our relations as regards the provision by Memo Bank, in its capacity as tied agent of Twenty First Capital, a portfolio management company authorised by the French Financial Markets Authority (*Autorité des Marchés Financiers*) under number GP-11000029, to the Client, of the Services.

They cancel and replace, as from their date of entry into force, any prior agreement entered into between the parties, whether written or oral, having the same subject matter.

The IS Terms form an indivisible whole with:

- the General Terms and Conditions, including their schedules (available at this address: https://memo.bank/convention);
- the Fee Schedule.

Terms beginning with a capital letter (for example: Account) are defined in the glossary in the General Terms and Conditions and in the article "Definitions".

In the event of contradiction between the terms of these IS Terms and those of the General Terms and Conditions, the terms of the latter shall prevail.

Only Clients meeting the eligibility criteria defined by Memo Bank may benefit from the Services under these IS Terms.

We also invite you to supplement your reading with our online help centre.

The provisions of these IS Terms may be updated by Memo Bank and such update will be the subject of a publication on our website. The Client shall be informed of such update.

It is recalled that, on simple request to Memo Bank, the retail Client, within the meaning of Directive 2014/65/EU, may be provided with a paper version of these IS Terms and of all information relating to the Investment Services, including the KID, the Prospectus and the suitability statement. Save for express disagreement on the part of the retail Client, the information will then be transmitted electronically after a period of eight weeks.

Any product or service not expressly provided for by the IS Terms shall be the subject of a specific and separate contract.

D.2. General warning

Before subscribing to a Financial Instrument, the Client must take note of the regulatory disclosure documents made available by Memo Bank (key information document for the investor, or "KID", and Prospectus), and of the risks attached to the investment envisaged.

It is recalled that past performance is not a guarantee of future performance, and the value of an investment may go up as well as down. Any investment in Financial Instruments may generate losses up to the totality of the capital invested.

Access to the investments offered by Twenty First Capital is available only in France and may be subject to restrictions vis-à-vis certain Clients, in particular as part of anti-money laundering and counter-terrorist financing procedures.

D.3. Definitions

AMF	French Financial Markets Authority (*Autorité des Marchés Financiers*).
Client	A client of Memo Bank, holder of an Account, and meeting all the eligibility criteria set unilaterally and exclusively by Memo Bank.
Investment Advice	Investment service defined by Article D. 321-1, 5°, of the French Monetary and Financial Code as the act of providing personalised recommendations to a third party, either at their request or at the initiative of the firm providing the advice, regarding one or more transactions in Financial Instruments or on one or more units mentioned in Article L. 229-7 of the French Environmental Code.
Confirmation	Document providing information relating to the execution of a Transaction initiated by the Client, issued by Twenty First Capital.
KID	Key information document covered by Regulation (EU) No 1286/2014 of 26 November 2014 on key information documents for packaged retail and insurance-based investment products and its subsequent implementing texts, as amended from time to time. It is systematically made available to the Client in their Workspace at the time of investment advice.
Directive 2014/65/EU	Directive of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments ("MiFID II"), as amended.
Financial Instruments	Financial instruments referred to in Article L. 211-1 of the French Monetary and Financial Code and in particular the units or shares of collective investment undertakings, the list of which is provided in the Appendix.
Working Day	Any day on which Memo Bank's offices are open.
Complaint Handling Procedure	Procedure under which Memo Bank handles complaints sent by its Clients.
Prospectus	Regulatory document including all information and characteristics relating to a collective investment undertaking (CIU).
Service(s)	The services covered by these general terms and conditions, namely the Investment Services and the Relational Service.
Investment Services	The investment services that the Provider may provide to the Client and which are the subject of these IS Terms, namely Investment Advice.
Relational Service	The introduction service for the purposes of subscription and redemption of Financial Instruments between the Client and Twenty First Capital, through Memo Bank, in accordance with the provisions of clause D.8, "Relational Service" of these IS Terms.
Transaction	Any operation of purchase, sale, placement or subscription of Financial Instruments.
Twenty First Capital	Portfolio management company authorised by the French Financial Markets Authority under number GP-11000029, having appointed Memo Bank as its tied agent.

D.4. Subject matter

The purpose of these IS Terms is to define the conditions under which Memo Bank may provide to the Client the Investment Service(s) relating to Financial Instruments as tied agent of Twenty First Capital.

The list of Financial Instruments is set out in the Annex and may be amended periodically and unilaterally by Memo Bank, which the Client accepts.

However, Memo Bank reserves the right, at its sole discretion, to refuse any Transaction relating to Financial Instruments in which it is prohibited from dealing under statutory or regulatory provisions that would expose it to sanctions, or in the event of material technical impossibility.

D.5. Authorised agents and representatives

The Client's Representative is the only person authorised to give instructions on its behalf.

The Client shall notify the Provider in writing as soon as possible of any change concerning the list of the authorised Representative(s).

It is the Client's responsibility to verify that any person it authorises to act on its behalf, and who may, as a result, engage its liability, has sufficient knowledge of the regulations applicable to the Financial Instruments in which that person intervenes on its behalf.

D.6. Classification of the Client

Pursuant to the regulations, the Client is informed that it shall be classified by separate act in one of the following categories by Memo Bank, within the meaning of Directive 2014/65/EU:

– retail clients;

– professional clients; or

– eligible counterparties.

The Client is informed of its right to request a different classification from that defined by Memo Bank.

However, it is for Memo Bank ultimately to accept or refuse the Client's reclassification request.

The conditions under which such request may be made by the Client, and the consequences that would result for its degree of protection, are those set out in Articles D. 533-4 et seq. of the French Monetary and Financial Code.

D.7. Investment Advice and assessment of the suitability of Investment Advice

Memo Bank, as tied agent of Twenty First Capital, is authorised to provide the Investment Service of Investment Advice to the Client.

In this context, Memo Bank must assess the knowledge and experience of the Client as regards the Investment Services and the Financial Instruments, as well as its financial situation and investment objectives, including its risk tolerance and ability to bear losses and its sustainability preferences.

The Client is duly informed that, where it does not communicate all the necessary information, or where, in the light of its profile, the investment in the relevant Financial Instrument is not suitable to its situation, Memo Bank shall provide it with a warning on a durable medium, before it carries out a Transaction.

Where Memo Bank provides Investment Advice to a retail Client, within the meaning of Directive 2014/65/EU, a suitability statement shall be provided to the Client prior to the Transaction. The suitability statement formalises the Investment Advice and explains why the recommendation made is suitable for the Client.

This statement presents a summary of the advice given and explains why the recommendation made is suitable for the retail Client, including the way in which it is in line with the Client's objectives and particular situation as regards the required investment period, the Client's knowledge and experience and the Client's attitude to risk and ability to bear losses. This suitability statement shall contain the information on the costs and related charges provided for in clause D.13, "Remuneration, costs and related charges", as well as the regulatory warning where applicable.

Where the Provider provides the service of Investment Advice to a Professional Client or an eligible counterparty within the meaning of Directive 2014/65/EU, Memo Bank may presume that the Client has the necessary knowledge and experience and is financially able to bear any risk associated with its investment objectives.

Furthermore, where Memo Bank provides Investment Advice on an ongoing basis, it shall send the Client an annual assessment of the suitability of the Financial Instruments it has recommended in light of its investment profile.

The Client is informed that Memo Bank provides the Investment Advice service on a non-independent basis, which entitles it to retain the remuneration received from Twenty First Capital, in compliance with the conditions provided for that purpose by the regulations.

The Financial Instruments that are the subject of the recommendation are issued or offered by Twenty First Capital, with which Memo Bank maintains close legal and economic links.

When it provides the Investment Advice service, the Financial Instruments that are the subject of the recommendation are subject to a restricted and limited analysis by Memo Bank and do not represent a complete range of the financial instruments available on the financial markets.

In connection with the provision of Investment Advice, and in compliance with the MiFID regulations, Memo Bank may receive a commission from Twenty First Capital.

D.8. Relational Service

Memo Bank provides its Clients with Investment Advice and offers, in this context, a Relational Service.

For the purposes of these IS Terms, the Relational Service is intended to put the Client and Twenty First Capital in contact, in order to collect Clients' requests for subscription and redemption of Financial Instruments with Twenty First Capital, and to follow up on their investments.

The Relational Service allows Clients to access online financial information and links to websites published by third parties. Memo Bank has not verified the completeness and/or currency of the third-party sites referenced or which link to Memo Bank's site.

Access to this information implies the prior and unreserved acceptance of these IS Terms.

D.9. Obligations and liabilities of Memo Bank

In compliance with the laws and regulations in force, Memo Bank and its staff act in accordance with the usages and practices of the profession.

Memo Bank is bound, in connection with the performance of this contract, by a best-efforts obligation.

It thus ensures that the resources implemented comply with the requirements imposed by the competent authorities and meet the technical standards in force for the activities concerned.

In accordance with Article L. 545-2 of the French Monetary and Financial Code, Twenty First Capital, Memo Bank's principal, remains fully and unconditionally liable vis-à-vis third parties for the acts performed in its name and on its behalf by Memo Bank and for the latter's omissions.

Save for the cases of limitation or exclusion of its liability set out in these IS Terms, Memo Bank shall in no way be liable for:

- losses or damages resulting from actions, omissions or delays in execution attributable to the Client, or which are the result of errors, negligence or misconduct by the Client's directors, officers, employees or representatives;
- losses or damages resulting from the incorrect transmission, lack of transmission or late transmission of messages or instructions by the Client, due to breakdowns or failures of the Client's own technical means of transmission, as well as cases of force majeure as defined by the French courts, of general blocking of communications, telecommunications or means of transport, or any other similar case;
- losses or damages resulting from the consequences of any failure, interruption, inaccuracy, slowdown, delay in execution or non-execution of all or part of its obligations hereunder as a result of any act, event or circumstance caused by the occurrence of a case of force majeure as defined by the French courts, including but not limited to strikes, failures of IT systems or means of communication;
- losses or damages resulting from the application of any law, decree, regulation or decision — including any exchange controls — promulgated or taken by the French authorities or those of the country in which the assets recorded or pending recording in the Clients' accounts are held, or by any governmental authority, political subdivision, public institution or institution — including the Central Bank — thereof; and
- any fault other than those that may be qualified as gross negligence or wilful misconduct committed by Memo Bank.

D.10. Obligations of the Client

The Client declares that it has been duly incorporated under the regulations applicable to it, and that it has full legal capacity to accept these IS Terms.

The Client undertakes to comply with the French and foreign regulations applicable to it or applicable to the IS Terms.

In particular, it undertakes to initiate only Transactions that comply with its articles of association and in particular with its corporate purpose.

In addition to the information undertakings made elsewhere under the General Terms and Conditions, the Client shall immediately inform Memo Bank, where applicable, of:

- any change in its legal form;
- any change in the composition of its reference shareholding or of its directors or legal representatives, providing in particular for this purpose an updated extract of the trade and companies register;
- any event modifying its capacity to act;
- any investigation or decision by its supervisory authorities, likely to result in due course in the suspension or withdrawal of all or part of its authorisation or leading it before a disciplinary, professional or administrative panel;
- any prosecution or conviction handed down, by a court (judicial, administrative or arbitral) or a disciplinary, professional or administrative panel, against itself, its directors or their collaborators in respect of activities carried out under these IS Terms or any other agreement, contract or convention having consequences on the application of these IS Terms; and
- any event likely to substantially affect its financial capacity.

The Client shall send Memo Bank all elements likely to give an account of its financial situation, and in particular its updated and certified financial statements where applicable.

The Client undertakes not to dispute any Transaction carried out at the initiative of one of its legal representatives, agents, employees or duly authorised delegatees, whose cessation of duties or mandate has not been duly notified to the Provider.

The Client undertakes to indemnify Memo Bank on first demand for any expenses, charges and damages that the latter may incur directly or indirectly, as well as to assist it in the event of claims, legal actions or other liability proceedings brought by a third party arising from a breach by the Client of any of its obligations under these IS Terms.

D.11. Confidentiality

In accordance with the regulations, Memo Bank is bound by professional secrecy.

However, that secrecy may be waived, in accordance with the law, in particular at the request of the supervisory authorities, the tax or customs authorities, and pursuant to a judicial act enforceable in criminal proceedings.

In addition, by way of derogation from the obligation of professional secrecy, the Client authorises Memo Bank to communicate any relevant information concerning it to Twenty First Capital, whose intervention is necessary for the execution of orders, or to its statutory auditors, legal advisers and insurers.

The Client is required to keep confidential all information received from the Provider under these IS Terms.

Finally, the parties acknowledge that their staff are bound to respect confidentiality on all the Transactions handled and refrain from any use and any exploitation, beyond the needs of these IS Terms, of the information they may become aware of.

D.12. Suspicious transactions

Memo Bank may in particular, pursuant to the legislation and regulations on the fight against money laundering and the financing of terrorism, require the Client to provide any information it deems necessary in respect of Transactions appearing unusual to it because of, in particular, their arrangements, their amount, their exceptional nature with regard to those handled until then, or for any other reason.

The Client undertakes to provide Memo Bank with any useful information on the context of its Transactions.

Furthermore, Memo Bank and its principal, Twenty First Capital, may make a report of suspicious transactions to the French Financial Markets Authority for any Transaction that Twenty First Capital would consider as constituting market abuse, in accordance with the regulations in force.

In such case, the Client will not be informed of this report by Memo Bank.

D.13. Remuneration, costs and related charges

Memo Bank's remuneration due by the Client in respect of the Investment Services provided by Memo Bank shall be communicated to the Client by separate act by Twenty First Capital and made available in the Workspace.

In connection with the provision of Investment Services to the Client, Memo Bank shall be remunerated by retrocessions of fees paid by Twenty First Capital, on the average of the daily amounts invested.

In addition, the Client may bear certain of the costs and charges related to the Financial Instruments levied on its investment by Twenty First Capital (for example, management fees and administrative charges). A reasonable estimate of the costs and charges is provided to the Client before the carrying out of the Transaction or the provision of the Investment Service.

In accordance with Article 50 of Delegated Regulation (EU) 2017/565, Memo Bank shall provide the Client, in a specific document, with all information relating to the costs and charges related to the Investment Services/product(s) it provides to the Client.

D.14. Communications/notifications

Memo Bank shall send the Client the Confirmations prepared by Twenty First Capital in French relating to the units or shares of CIU in which it has invested.

Any information that must be provided to the Client by Memo Bank under these IS Terms or the regulations in force may in particular be transmitted by email or via a publication on Memo Bank's website or in the Workspace.

D.15. Management of conflicts of interest

Memo Bank implements, under the conditions provided for by the regulations, an effective policy for managing conflicts of interest, which is published on the website of Memo Bank's principal (Twenty First Capital).

D.16. Telephone and electronic recordings — Means of evidence

For the purposes of the proper performance of the IS Terms, the Client expressly authorises the recording of all its telephone and electronic conversations with Memo Bank and its staff.

Telephone conversation recordings are not necessarily preceded by an audible warning.

The Client also authorises Memo Bank and its staff to record on a durable medium any relevant information relating to their conversations.

These recordings shall be available on request for five years and, if the French Financial Markets Authority so requests, for seven years.

In addition to the information contained on a durable medium, all forms of recording resulting from the means of communication used between the Client and Memo Bank, and in particular the telephone recordings and electronic messages made and sent by Memo Bank, are admissible as means of evidence and shall be authoritative, in particular in the event of litigation.

The Client acknowledges that any Transaction carried out via an electronic system shall be deemed to manifest the Client's consent to that transaction; that consent shall have the same value as consent given in writing.

D.17. Processing of personal data

Memo Bank, in its capacity as tied agent of Twenty First Capital, collects personal data concerning its Clients and their legal representatives and beneficial owners as processor on behalf of Twenty First Capital.

Twenty First Capital shall also collect and process personal data of the Clients.

The personal data thus collected and processed under the General Terms and Conditions, Special Terms and Conditions and Fee Schedule are necessary:

- for their conclusion and execution; for compliance with and execution of Memo Bank's legal and regulatory obligations;
- for the pursuit of its legitimate interests.

The Client declares that it has taken note of and accepted the Memo Bank Personal Data Protection Policy, which describes the purposes of the processing of personal data collected, the arrangements for its communication to third parties, the rights relating to such data and the security measures put in place.

It is recalled that the persons concerned have the rights of access and information, rectification and erasure of their personal data.

They may exercise these rights at any time and free of charge, at a reasonable interval, with the data protection officer by email at the following address: protectiondesdonnees@memo.bank.

They may, in the event of a dispute, contact the French Data Protection Authority (CNIL).

To refer the matter to the CNIL, a simple letter should be addressed to the attention of the president of the CNIL, Commission nationale de l'informatique et des libertés — 3, Place de Fontenoy — TSA 20715 — 75334 Paris Cedex 07.

D.18. Term and termination of the IS Terms

The IS Terms are concluded for an indefinite term and are deemed to have been accepted by the Client as soon as a Service has been provided by Memo Bank to the Client.

They may be terminated at any time by the Client or Memo Bank subject to 30 (thirty) calendar days' notice.

The Transactions in progress, once termination has taken effect, shall continue to be governed by the provisions of these IS Terms.

The IS Terms may be terminated by operation of law, without formal notice, by Memo Bank by notification of termination by registered letter with acknowledgement of receipt, in the following cases:

- effective termination of the services agreement;
- amicable dissolution of the Client provided for by law;
- serious misconduct on the part of the Client (for example: illegal activities, fraudulent conduct or false declarations); and
- loss, withdrawal, suspension or non-renewal of an authorisation, approval, licence, registration in a professional register, financial guarantee, regulated surety or any other compulsory insurance required for the conduct of your activity.

Such termination takes effect upon receipt of such letter by the Client and entails the cessation of the provision of the Services by Memo Bank to the Client. For the purposes of this article, receipt of a registered letter with acknowledgement of receipt by the Client to whom it is addressed shall be understood as the date of first presentation of such letter.

The Client shall then be invited to contact Twenty First Capital once the IS Terms have been terminated, in order to take a decision regarding the Financial Instruments held.

D.19. Complaint handling

Complaints against the conditions of performance of the Services must be sent to Twenty First Capital, Memo Bank's principal, from the event giving rise to the complaint.

Complaints must be made in writing and reasoned.

Any complaint sent by post must be addressed to the Secretary General — RCCI of Twenty First Capital at the postal address: 39, Avenue Pierre 1er de Serbie, 75008 Paris, France. Complaints may also be sent to the following email address: chrys.iliou@twentyfirstcapital.com or to your usual contact within the Twenty First Capital management company (https://www.twentyfirstcapital.com/).

They are handled by Twenty First Capital in accordance with the Complaint Handling Procedure, which is made available free of charge to the Client on Twenty First Capital's website pursuant to the regulations in force.

D.20. Appendix: List of Concerned Financial Instruments

In accordance with the "Purpose" article of these Investment Services Terms and Conditions, you will find below the list of funds and compartments managed by Twenty First Capital to which these general terms and conditions of investment services apply.

Fund Name	Regulatory Category	Sub-fund Name	Share Class	ISIN Code
Spiko SICAV	UCITS	Spiko US T-Bills Money Market Fund	Action USD	FR001400ODM9
Spiko SICAV	UCITS	Spiko US T-Bills Money Market Fund	Action EUR	FR001400SBD3
Spiko SICAV	UCITS	Spiko EU T-Bills Money Market Fund	N/A	FR001400ODL1
Spiko SICAV	UCITS	Spiko Amundi Overnight Swap Fund	Action EUR D	FR0014017WQ8
Spiko SICAV	UCITS	Spiko Amundi Overnight Swap Fund	Action USD D	FR0014017WR6
Spiko SICAV	UCITS	Spiko Amundi Overnight Swap Fund	Action GBP D	Pending*
Spiko SICAV	UCITS	Spiko UK T-Bills Money Market Fund	Action GBP	FR0014012MN7
Spiko SICAV	UCITS	Spiko UK T-Bills Money Market Fund	Action EUR	FR0014012MO5

* Distribution of this share class may only begin after the ISIN code has been assigned.

The commercial names "Amundi STAR EUR", "Amundi STAR USD" and "Amundi STAR GBP" refer, respectively, to the EUR D, USD D and GBP D shares of the Spiko Amundi Overnight Swap Fund sub-fund listed above.

Schedule E: Terms of use of the Premium API

E.1. Presentation of the Premium API

The Premium API is an Application Programming Interface that allows you to access data and documents stored in your Workspace and to carry out operations by connecting your own IT infrastructure to your Workspace.

The Premium API allows you in particular:

- to consult the information relating to your Accounts;
- to consult the information and attachments relating to Payment Transactions debiting and crediting your Accounts;
- to attach supporting documents to Payment Transactions;
- to receive notifications of events such as Payment Transactions carried out on your Accounts or the creation of Virtual IBANs;
- to initiate Credit Transfers;
- to create or delete Virtual IBANs.

E.2. Activation of the Premium API

The use of the Premium API is reserved for customers whose subscription expressly provides for its application.

It is the subject of specific invoicing in accordance with the Fee Schedule.

E.3. Sandbox

We make available to you a test environment (Sandbox) reproducing the main features of the API in production. You may thus test the integration with the API and simulate different usage scenarios.

As the Sandbox is provided for development and testing purposes only, it does not allow real Payment Transactions of binding legal value to be carried out. The features and data available in the Sandbox may thus differ from those of the production environment.

We do not guarantee permanent availability of the Sandbox and may modify or suspend it at any time.

We disclaim all liability in the event of damage resulting from the use of the Sandbox, in particular if functional configurations in this environment prove to be non-operational in production.

E.4. Users — Powers of Attorney

Only the Representative may access the Workspace to activate the Premium API.

However, the Representative may grant a Power of Attorney to one or more Users for that purpose. The Power of Attorney must be granted by the Representative or by an authorised User within the Workspace, where the steps to be followed are specified.

We reserve the right not to approve a User or to revoke its approval at any time, without prior notice or justification, without such decision giving rise to any liability on our part.

Any User may at any time revoke a Power of Attorney granted in the Workspace.

Each User authorised to use the Premium API shall use unique and personal identification keys, available in the Workspace, to identify themselves.

Operations carried out through the Premium API are not performed by a robot or machine, but by an authorised and identified User.

They bind you as if you had carried them out yourself.

You may also authorise a Partner to use the Premium API.

You acknowledge that the use of the Premium API relies on strong authentication mechanisms at the initial configuration of the connection or the generation of the access keys.

Accordingly, you accept that any Payment Order received by Memo Bank via the Premium API, where it uses the valid technical credentials of the Partner you have authorised, is deemed to have received your consent.

E.5. Your responsibility

The operations you carry out through the Premium API are carried out in your name and produce the same legal effects as an action carried out in the Workspace.

It is your responsibility to implement an appropriate and effective information security policy and to train your staff in security best practices.

In this respect, it is for you in particular:

- to take all necessary measures to prevent and address any breaches of your information system by third parties;
- to comply with all laws and regulations in force;
- to use the Premium API in accordance with the technical documentation accessible from the Workspace and at https://docs.api.memo.bank/;
- to ensure the strict confidentiality of your Personalised Security Credentials and your identification keys, which must under no circumstances be communicated to third parties;
- to use IT equipment in compliance with the state of the art as regards security.

Accordingly, you shall refrain from:

- circumventing the security rules or technical limits of the Premium API;
- using the Premium API to provide payment services to your own customers;
- exceeding a reasonable number of requests beyond which the proper functioning of the Premium API could be disrupted; we may, depending on the use you make of our services, ask you to comply with limits on calls to the API;
- selling or renting the Premium API to third parties;
- carrying out reverse engineering.

You thus undertake to indemnify us for any loss arising from non-compliant use of the Premium API. We shall not be liable for malfunctions resulting, directly or indirectly, from a breach of your obligations or from the act of a third party.

E.6. Personal data

We may collect personal data concerning you in connection with the use of the Premium API.

We invite you in this respect to consult the Memo Bank Personal Data Protection Policy, which describes the purposes of the processing of the personal data collected, the arrangements for its communication to third parties, your rights relating to such data and the security measures put in place.

Schedule F: Service Level Agreement

F.1. Subject matter

The service level agreement (hereinafter the "SLA") defines Memo Bank’s commitments in terms of availability of the Premium API and of customer support.

It applies to Memo Bank’s customers whose subscription expressly provides for its application (hereinafter referred to as the "Client" or "Clients").

F.2. Definitions

Term	Definition
API	This is the Premium API, an application programming interface made available by Memo Bank allowing Clients to access services and carry out operations on their Memo Bank accounts.
Client	Any legal entity that has subscribed to a Memo Bank subscription including access to the Premium API and providing for the application of the SLA.
Non-critical Incident	Any event resulting in a service interruption or unavailability which is not a Critical Incident.
Critical Incident	System malfunction preventing the Client from carrying out a task essential to its business and for which there is no workaround.
Unavailability	Period of more than 5 minutes during which all requests to the API are rejected with an HTTP 5xx error code (server error).
Scheduled Maintenance	Periods announced two weeks in advance during which the API is rendered unavailable for updates, improvements or maintenance operations.
API Request	All requests made through the API. The price of requests is specified in the Fee Schedule.
Business Hours	Monday to Friday from 9:00 a.m. to 5:00 p.m., Paris time (CET), excluding public holidays in France.

F.3. Service commitments

F.3.1. Service availability

Memo Bank undertakes to guarantee an API availability of 99.9% per calendar month, excluding Scheduled Maintenance periods and the cases provided for in clause F.4, “Exclusions”.

The status of the API and any incidents can be consulted on the Memo Bank help website (https://aide.memo.bank/article/371-etat-api-incidents).

F.3.2. Customer support

Memo Bank's customer support is accessible from the messaging integrated into the Memo Bank workspace, and by email at support@memo.bank. There is no telephone support available.

Memo Bank undertakes to respond, during Business Hours, to all requests sent to customer support within the following time limits:

Type of request	First response time of support
Critical Incident	≤ 2 hours
Non-critical Incident	≤ 4 hours
Other requests	≤ 4 hours

F.4. Exclusions

F.4.1. General principle

Memo Bank's commitments set out in this SLA do not apply to interruptions, slowdowns, access difficulties or other performance issues of the Premium API caused by circumstances beyond Memo Bank's reasonable control, in particular if the unavailability of the API is exclusively attributable to a third party.

F.4.2. Specific exclusions

Memo Bank shall not be liable in the following cases, this list not being exhaustive:

Category	Examples of exclusions
Actions of the Client	– Errors or omissions in the Client's code – Use of obsolete API versions – Non-compliance with the usage limits and quotas defined by Memo Bank – Use of the API in a manner not complying with the documentation
Failures of third-party infrastructure	– Unavailability or malfunction of cloud providers' services – Outages or slowdowns of telecommunications networks – Failures of Internet service providers

Network issues	– Total or partial unavailability of the Internet network – Widespread slowdowns of Internet communications
Malicious attacks	– Denial-of-service attacks (DDoS) – Other types of attacks targeting the Client, Memo Bank or the infrastructure used
Force majeure events	– Natural disasters – Armed conflicts – Governmental or regulatory decisions affecting the provision of the service
Maintenance	Scheduled Maintenance periods

F.4.3. Client's notification obligation

The Client undertakes to notify Memo Bank as soon as possible if it finds an interruption or degradation of the service that may fall within the exclusions mentioned above.

Such notification will enable Memo Bank to investigate promptly and, where applicable, to take the necessary steps to restore the service or mitigate the impact of the Incident.

F.5. Indemnification

If the availability of Memo Bank's API is lower than the thresholds defined below, Memo Bank shall pay the Client, as a lump-sum and final penalty clause, an indemnification calculated as a percentage of the amount excluding tax of the fees paid by the Client during a given month in respect of API requests in accordance with the following table:

API availability (%)	Penalties (%)
< 99.9% and ≥ 99%	5%
< 99% and ≥ 95%	15%
< 95%	25%

If the first response time of customer support exceeds the times mentioned in clause F.3.2, "Customer support", Memo Bank shall pay the Client, as a lump-sum and final penalty clause, an indemnification calculated as a percentage of the amount excluding tax of the entire invoice for a given month in accordance with the following table:

Type of request	First response time of support	Penalties (%)
Critical Incident	> 2 hours	5%
Critical Incident	> 4 hours	10%

Non-critical Incident	> 4 hours	10%
Other requests	> 4 hours	10%

In all cases, the Client must send its indemnification requests to its account manager, accompanied by all useful supporting documents, within 15 days following the end of the month during which an Unavailability was noted.

Such indemnification shall then be paid into the Client's Principal Account.

F.6. Limitation of liability

The maximum amount of indemnifications that may be paid to a Client in respect of the Unavailability of the API for a given month may not exceed 25% of the amount of fees paid by the Client during the same month in respect of API requests.

The maximum amount of indemnifications that may be paid to a Client in the event of non-compliance with the first response time of customer support for a given month may not exceed 25% of the amount of all fees relating to the subscription and to API requests paid by the Client during the same month.

Memo Bank shall not be liable for any indirect or consequential damage resulting from the use of, or the impossibility of using, the API, including, but not limited to, loss of business, loss of data and any financial or commercial loss.

F.7. Security

F.7.1. General commitment

Memo Bank undertakes to implement and maintain security measures in accordance with the state of the art to protect Clients' data and ensure the confidentiality, integrity and availability of the API.

Such measures are designed to prevent unauthorised access, disclosure, alteration or destruction of the data processed by the API.

F.7.2. Management of security incidents

In the event of a security incident affecting the API or the Clients' data, Memo Bank undertakes to:

- inform the Clients concerned as soon as possible after the discovery of the incident;
- conduct a thorough investigation to determine the cause and extent of the incident;
- take the necessary steps to resolve the incident and, where applicable, cooperate with the third parties concerned to restore the service as soon as possible.

F.7.3. Training and awareness

Memo Bank provides ongoing security training for all its staff. These training and awareness actions are provided to all employees, whether or not involved in the development, maintenance and operation of the API.

F.7.4. Protection of personal data

Memo Bank undertakes to comply with the applicable data protection regulations, in particular the General Data Protection Regulation (GDPR), in accordance with its personal data protection policy.

F.8. Termination

This SLA forms an indivisible whole with the services agreement, which the Client expressly acknowledges having read and accepted.

Accordingly, any termination of the services agreement shall entail, by operation of law, termination of the SLA.

Likewise, as set out above, the clauses of this SLA apply only to Memo Bank's customers whose subscription expressly provides for its application.

Therefore, any change in subscription plan may entail termination of the SLA.

F.9. Amendment of the SLA

This SLA may be amended at any time, at the initiative of Memo Bank, under the same conditions as amendments to the services agreement.

Schedule G: Terms of use of Click to Pay

G.1. Presentation of Click to Pay

Click to Pay is a service associated with your Visa Cards (physical and virtual) which aims to simplify and secure your online purchases by replacing the manual entry of your banking details with an automated and secure payment process, recognisable by the Click to Pay logo (a symbol depicting an arrow pointing to the right) on compatible merchant sites.

Click to Pay uses "tokenisation" technology to protect the information of your Cards.

This technology replaces the actual Card data with a unique digital token during transactions, thereby reducing the risk of fraud.

Payment Transactions carried out via Click to Pay are considered to be classic Payment Transactions by Card and are subject to the same operating and pricing rules as those defined in the Agreement.

G.2. Activation

Click to Pay is a feature activated by default with your Visa Cards.

In this respect:

– for new Cards: any new Card (physical or virtual) issued by Memo Bank is automatically enrolled in the Click to Pay service from the time of its creation;

– for existing Cards: your current Cards are automatically enrolled in the Click to Pay service by us.

This automatic enrolment creates your Click to Pay profile and associates your Cards with it, using the data (email, telephone number) associated with the Cardholder in the Workspace.

G.3. Management of the service and right to opt out

Although Click to Pay is activated by default to facilitate your payments, the Cardholder may at any time, and free of charge, decide no longer to benefit from this service for one or more of their Cards. Such deactivation is carried out directly from the Workspace.

The Cardholder may reactivate the service at any time from their Workspace.

G.4. Consent of the Cardholder to make a payment using Click to Pay

When a Cardholder uses Click to Pay to settle an online purchase, we consider that their agreement is firm and irrevocable as soon as they:

– select their Memo Bank Card in the Click to Pay interface on the merchant's website;

– confirm the transaction, where applicable, by a security measure (such as entering a one-time code received by SMS or email, or by Strong Customer Authentication via the mobile application).

G.5. Updating of data

The proper functioning of Click to Pay depends on the accuracy of the Cardholder's contact details (in particular the email address and mobile phone number).

As the issuer managing the service, Memo Bank automatically updates your Click to Pay profile when you change your contact details in the Workspace.

Likewise, in the event of renewal or replacement of your Card (following expiry, loss or theft), we automatically ensure the updating of the new information in Click to Pay, unless you had previously deactivated the service for that Card.

Schedule H: Terms of use of the Partners API (Marketplace)

H.1. Subject matter

This Schedule defines the conditions under which a Partner is authorised to connect its software solution to Memo Bank's infrastructure in order to be listed on the Marketplace and to offer its services to Memo Bank's customers.

The Partner acknowledges that it is authorised to access data and to transmit instructions only after having received an express and prior mandate from a customer holding an account with Memo Bank and a user of the Partner's solution (hereinafter the "Common Customer") via the authorisation protocol implemented by Memo Bank.

H.2. Role of the Partner and routing of flows

In this context, the Partner acts as a technical intermediary between the Common Customer and Memo Bank.

It undertakes to:

- respect the integrity of the instructions (including Payment Orders) initiated by the Common Customers on its interface and to transmit them unchanged to Memo Bank;
- retrieve only the account data strictly necessary for the provision of the service promised to the Common Customers;
- clearly inform the Common Customers of the scope of the technical authority they grant it on activation of the connection;
- at no time take possession of the funds belonging to the Common Customers nor exercise any control over them.

H.3. Protection of personal data

The Partner acts as an independent controller of the personal data it receives through this connection.

It undertakes to process such data in accordance with the applicable data protection regulations and to make available to the Common Customers an accessible privacy policy describing the processing it operates.

In the event of revocation of access by the Common Customer, the Partner undertakes to cease all processing of the data received and to delete it within a reasonable period, unless required by law to retain it.

H.4. Security and integrity of accesses

The security of the connection relies on the protection of the technical accesses (API keys, authentication tokens) delegated by the Common Customers.

The Partner undertakes to implement technical and organisational security measures in accordance with the state of the art in order to protect its infrastructure against any intrusion or misuse.

Any security incident occurring on the Partner's platform and liable to affect the data or funds of the Common Customers must be notified to Memo Bank without delay so that accesses may be immediately revoked.

H.5. Liability of the Partner

The Partner assumes full responsibility for the instructions transmitted via its own tools.

Memo Bank shall not be liable for the consequences of a Payment Order transmitted by the Partner if that Order complies with the technical accesses configured by the Common Customer.

In the event of a processing error, undue transmission or fraud resulting from a failure of the Partner's solution, the latter shall indemnify Memo Bank against any claim from the Common Customers or any resulting financial loss.

H.6. Listing on the Marketplace

The Partner's listing on the Marketplace is a simple promotion of the technical compatibility between the two solutions.

It does not constitute an approval by Memo Bank of the quality of the Partner's services.

Memo Bank reserves the right, at its sole discretion, to suspend access to its APIs or to withdraw a Partner's listing on the Marketplace without notice in the following cases:

- established or suspected risk to the security of customers' funds or data;
- breach of these terms;
- repeated negative feedback or complaints from common customers.

H.7. Intellectual property and communication

Memo Bank and the Partner may publicise their collaboration to promote the interconnection to the Common Customers.

Throughout the term of the Marketplace listing, the Partner authorises Memo Bank to use its name and distinctive signs (logo, trademark) free of charge to promote the interconnection and display its solution on Memo Bank's communication materials.

Reciprocally, the Partner is authorised to use the Memo Bank logo exclusively to signal such technical compatibility to its customers, in compliance with Memo Bank's brand guidelines.

Any other use of the Memo Bank trademark by the Partner, or any communication suggesting a partnership beyond mere technical interconnection, is subject to Memo Bank's prior written agreement. Each party remains the owner of its intellectual property rights.

Schedule I: General information on the protection of deposits

The general principle is that all customers, whether individuals or businesses, whether their accounts are opened in a personal or professional capacity, are covered by the Deposit Guarantee and Resolution Fund (FGDR). The exceptions applicable to certain deposits or to certain products are indicated on the FGDR's website. Memo Bank informs you on request whether its products are guaranteed or not. If a deposit is guaranteed, we also confirm this on the account statement sent periodically and at least once a year.

Protection of deposits made with Memo Bank is ensured by:	The Deposit Guarantee and Resolution Fund (FGDR)
Protection ceiling:	€100,000 per depositor and per credit institution [1]
If you have several accounts with the same credit institution:	All your deposits recorded on your accounts opened with the same credit institution falling within the scope of the guarantee are added together to determine the amount eligible for the guarantee; the amount of compensation is capped at €100,000 [1]
If you hold a joint account with one or more other persons:	The cap of €100,000 applies to each depositor separately. The balance of the joint account is divided among its co-holders; each share is added to that holder's own assets for the calculation of the guarantee ceiling that applies to them. [2]
Other special cases:	See note [2]
Compensation period in the event of failure of the credit institution:	Seven business days [3]
Currency of compensation:	Euros
Correspondent:	Fonds de garantie des dépôts et de résolution (FGDR) 65, rue de la Victoire, 75009 Paris Telephone: 01-58-18-38-08 Email: contact@garantiedesdepots.fr
For more information:	Please refer to the FGDR's website: http://www.garantiedesdepots.fr
Acknowledgement of receipt by the depositor:	Acknowledged on acceptance of the general terms and conditions of the Current Account agreement (but not when the annual form is sent).

1 General limit of protection: if a deposit is unavailable because a credit institution is unable to meet its financial obligations, depositors are compensated by a deposit guarantee scheme. Compensation is capped at €100,000 per person and per credit institution. This means that all credit accounts with the same credit institution are added together in order to determine the amount eligible for the guarantee (subject to the application of the statutory or contractual provisions on set-off with debit accounts). The compensation ceiling is applied to this total. The deposits and persons eligible for this guarantee are mentioned in Article L. 312-4-1 of the French Monetary and Financial Code (for any clarification on this point, see the website of the Deposit Guarantee and Resolution Fund). For example, if a customer holds an eligible savings account (excluding Livret A, Livret de développement durable and Livret d'épargne

populaire) with a balance of €90,000 and a current account with a balance of €20,000, compensation will be capped at €100,000. This method also applies where a credit institution operates under several trade marks.

2 Main special cases: joint accounts are divided between the co-holders in equal shares, save for any contractual stipulation providing for a different allocation. The share allocated to each is added to their own accounts or deposits and the resulting total benefits from the guarantee up to €100,000. Accounts on which at least two persons have rights as co-owners, partners of a company, members of an association or any similar grouping without legal personality are pooled and treated as having been made by a single depositor distinct from the co-owners or partners. Accounts belonging to a sole trader with limited liability (EIRL), opened in order to allocate the assets and bank deposits of their professional activity, are pooled and treated as having been made by a single depositor distinct from the other accounts of that person. The sums recorded on Livret A, Livret de développement durable (LDD) and Livret d'épargne populaire (LEP) accounts are guaranteed independently of the aggregate ceiling of €100,000 applicable to other accounts. This guarantee covers the sums deposited on all such savings accounts for the same holder, together with the interest relating to these sums, up to €100,000 (for any clarification, see the website of the Deposit Guarantee and Resolution Fund). For example, if a customer holds a Livret A and an LDD with a total balance of €30,000 as well as a current account with a balance of €90,000, they will be compensated, on the one hand, up to €30,000 for the savings accounts and, on the other hand, up to €90,000 for the current account. Certain exceptional deposits (a sum arising from a real estate transaction carried out on a residential property belonging to the depositor; a sum constituting compensation in capital for damage suffered by the depositor; a sum constituting payment in capital of a retirement benefit or an inheritance) benefit from an increase in the guarantee beyond €100,000, for a limited period following their receipt (for any clarification on this point, see the website of the Deposit Guarantee and Resolution Fund).

3 Compensation: the Deposit Guarantee and Resolution Fund makes compensation available to depositors and beneficiaries of the guarantee, for the deposits covered by it, within seven business days from the date on which the Prudential Supervision and Resolution Authority finds that the deposits of the member institution are unavailable pursuant to the first paragraph of I of Article L. 312-5 of the French Monetary and Financial Code. This seven-business-day period shall apply as from 1 June 2016; until that date, this period is twenty business days. This period concerns compensation that does not involve any particular processing or any additional information necessary for determining the amount that may be compensated or identifying the depositor. If specific processing or additional information is required, the payment of compensation shall occur as soon as possible. The making available is made, at the choice of the Deposit Guarantee and Resolution Fund: (i) either by the sending of a letter-cheque by registered post with acknowledgement of receipt, (ii) or by making the necessary information available online on a secure Internet area opened for that purpose by the Fund and accessible from its official website (see below), in order to enable the beneficiary to indicate the new bank account into which they wish the compensation to be paid by credit transfer.