Privacy Policy

Last updated on September 9, 2026

> **Unofficial translation.** This document is an unofficial English translation of Memo Bank's Privacy Policy.
>
> 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. General Provisions

Memo Bank is committed to protecting your personal data. This policy explains how we collect, use, store, and share your information when you use our services, in accordance with the General Data Protection Regulation (GDPR) and the French Data Protection Act (Loi Informatique et Libertés).

This Privacy Policy applies to any natural person whose data is collected and processed by Memo Bank, in particular in connection with using the website memo.bank (the "Site"), entering into any contract with Memo Bank, accessing the workspace client.memo.bank (the "Workspace"), using our other services—such as the iOS and Android mobile applications (the "Mobile Applications") on mobile devices—and using the Click to Pay online payment service as well as mobile payment services like Google Pay and Apple Pay.

The data controller is Memo Bank, whose contact details are set out in the legal notice of the Site. Our Data Protection Officer can be contacted at protectiondesdonnees@memo.bank.

As our customers are exclusively businesses, the data subjects concerned are in particular the legal representatives, beneficial owners, authorised agents and users of our customers, as well as the natural persons whose data appears in our customers' transactions and documents (employees, counterparties, contacts). Where we do not collect this data directly from you, it comes from our customer, from public registers and sources (trade and companies register, register of beneficial owners, sanctions lists, press) or from providers specialising in identity verification and anti-money laundering.

2. Collection of Personal Information

We may collect personal data in the following situations (non-exhaustive list):

- recruitment: a candidate submits an application in connection with recruitment;
- request to establish a business relationship: a user makes a request to establish a business relationship, in particular to open an account;
- partnership: a user submits a partnership request;
- newsletter: a user subscribes to our newsletter;
- social media: a user sends a private message via social networks;
- webinars: a user registers for a webinar hosted by Memo Bank;
- sales outreach: a user communicates with a sales representative by email or phone;
- indirect collection and B2B outreach: we may collect your professional data (last name, first name, job title, email address, phone number) indirectly through partners specializing in professional data enrichment or from public sources (such as professional social networks);
- other inquiries: a user sends an email to one of our generic email addresses;
- application review: a user submits supporting documents in the Workspace;
- use of the Workspace, the Mobile Applications, and our APIs;
- use of the Sandbox (our testing environment);
- use of the Click to Pay online payment service: a user uses their Memo Bank Visa card to pay for a purchase via the Click to Pay service;
- use of mobile payment services (Google Pay, Apple Pay): a user adds their Memo Bank card to a mobile payment application and uses it for in-store, online, or in-app payments;
- activation of a third-party tool from the Marketplace: when you connect a Partner to your Workspace, data regarding your Accounts and Payment Operations is transmitted to this Partner upon your express instruction;
- connection of a third-party artificial intelligence assistant through our MCP server: when you authorise, using the OAuth protocol, an AI assistant of your choice to access your Workspace, data regarding your Accounts and Payment Operations is transmitted to the provider of that assistant upon your express instruction (see Connecting to an AI assistant);
- signing and execution of the services agreement, loan agreements, and any other contracts entered into with Memo Bank;
- compliance with our legal and regulatory obligations and the pursuit of our legitimate interests.

In this context, we may collect the categories of data presented below, which include, but are not limited to, the following:

Category of data	Examples of collected data
Identification and professional data	– Last name and first name; – Date and place of birth; – Nationality; – Personal and professional address; – Personal and professional email address; – Landline and/or mobile phone number(s); – Profession and employment status; – Employer name and details (if applicable); – Identification numbers (SIRET, LEI, intra-community VAT, etc.); – Financial information (income, assets, etc.).

Category of data	Examples of collected data
Biometric data	Biometric data is used only in the following cases: – Qualified electronic signature: collected and processed via our certified provider Yousign when signing contractual documents that require a qualified electronic signature under the eIDAS Regulation; – Secure mobile device pairing: local biometric data (fingerprint or facial recognition) used on your device for Strong Customer Authentication (SCA) when accessing the Mobile Application, in accordance with the security requirements of the Payment Services Directive (PSD2); – Remote identity verification: biometric comparison between the photograph on the identity document and a capture of the face, carried out by Yousign (Youtrust) as part of its qualified electronic signature service at onboarding, pursuant to our legal obligations regarding anti-money laundering and countering the financing of terrorism (Article 9(2)(g) of the GDPR). This biometric data is never stored centrally by Memo Bank. For mobile pairing, it remains on your device and is managed by your phone's operating system (iOS or Android). For qualified electronic signatures, it is processed by Yousign in accordance with the eIDAS Regulation and deleted once the signing process is complete. For remote identity verification, only the outcome of the verification is retained by Memo Bank.
Account credentials and authentication data	– Login credentials (usernames, email addresses); – Passwords; – Secure access codes (authentication tokens, etc.).

Category of data	Examples of collected data
Payment data	– Bank account details (IBAN, BIC); – SEPA Direct Debit mandates; – Payment card details (card number, expiration date, security code/CVV); – Transaction history.
Data processed in connection with the national register of accounts reported for fraud risk (FNC-RF)	– Identifier of the reported account (IBAN or BBAN within the meaning of Regulation (EU) No 260/2012); – BIC code of the account-keeping institution; – Detection date; – Original channel of the fraudulent transaction (if applicable); – Fraud source — method used by the fraudster (if applicable); – Fraud category; – Transaction type; – Where applicable, the existence of a user claim or complaint regarding identity theft under Article 226-4-1 of the French Criminal Code.
Data processed as part of the Click to Pay service	– Identity data: last name, first name; – Contact details: email address, mobile phone number, billing address; – Card details: card number (PAN), expiration date; – Technical data: country code, technical customer ID, transaction timestamps.

Category of data	Examples of collected data
Service usage data	– Actions performed within the Workspace and Mobile Applications; – Connection logs (dates, times, IP addresses); – Pages visited on our website; – Interactions with emails and notifications; – Billing and contractual data.
Technical and logging data	– Technical identifiers assigned by Memo Bank to your Accounts, Payment Operations and Workspace users; – Technical logs of accesses made by an AI assistant connected to your Workspace through our MCP server: technical events (timestamp, technical identifiers of the client, user and connection, assistant identifier and version, requested operation, outcome) and technical content of requests and responses (access scopes, parameters received, data returned).
Supporting documents	– Identity documents; – Proof of address; – Commercial documents (invoices, contracts, etc.).

Category of data	Examples of collected data
Data relating to the fight against money laundering and terrorist financing	– Verified identity documents; – Proof of address; – Proof of funds origin; – Nature and purpose of the business relationship; – Risk profile; – Technical data collected when using our services (such as IP address, device model, operating system, connection timestamps, or interface interaction patterns); – Suspicious transaction reports (STRs), where applicable.

Data processed in connection with payment fraud prevention systems (FPAD and VOP services)	– As part of our participation in industry-wide fraud-detection systems designed to pool fraud detection resources, we process the following categories of data:
	  – Transaction data: information contained in payment transactions and related messages (IBAN, names of debtors/creditors, amounts, dates, etc.);
	  – Query data: information we submit to these services for analysis (e.g., an IBAN and name for verification purposes);
	  – Derived data: statistics, profiles, and statistical models generated by the service based on transaction and query data;
	  – Risk assessment outcomes: risk indicators and scores generated by the service in response to our queries.

Category of data	Examples of collected data
Recordings of sales conversations	– Audio and/or video recordings of sales interactions (outreach meetings, product demonstrations, follow-up calls) with our prospects and clients; – Associated metadata: date, time, duration, participant IDs, automated transcripts, and generated insights.

All collected information:

- will be processed fairly and lawfully;
- will be recorded for specific and legitimate purposes;
- will be used in accordance with those purposes;
- is adequate, relevant, and not excessive in relation to those purposes;
- will be protected by appropriate measures to ensure data security and confidentiality, preventing damage, modification, destruction, or unauthorized disclosure.

These data collections are strictly in compliance with applicable personal data protection regulations and are subject to appropriate security measures, detailed in the Security section.

3. Purposes and Legal Bases of Processing

We process your personal data for various purposes, each based on a specific legal basis. This processing is carried out for the following purposes:

Legal basis	Purposes of processing
Performance of our contractual obligations	– Providing access to the Workspace, bank accounts, and the Memo Bank API; – Providing, managing, and executing all payment methods and services made available to you, including credit transfers, direct debits, card payments, and access to digital payment services (Click to Pay, Google Pay, Apple Pay); – Providing assistance with the verification of your transaction payees by granting access to their public legal information (such as company name, SIREN number, etc.); – Billing for our services; – Implementing the security measures necessary to operate our services; – Informing the account holder of actions performed by users of the account; – Transmitting your Account and Payment Transaction data to Marketplace Partners, upon your express instruction and within the limits of the access rights you have granted them; – Transmitting your Account and Payment Transaction data to the provider of the third-party artificial intelligence assistant you have chosen to connect through our MCP server, upon your express instruction and within the limits of the access scopes you have authorised.

Legal basis	Purposes of processing
Compliance with our legal obligations	– Complying with legal and regulatory obligations (dispute resolution, risk management, fraud prevention); – Reviewing documents for current account openings or the granting of financing; – Biometric analysis of official identity documents; – Implementing transaction monitoring and screening systems to comply with our legal obligations regarding Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) and international sanctions; – Implementing the Verification of Payee (VOP) service in accordance with European instant payment regulations, to verify that the IBAN matches the name of the payee; – Registering information regarding accounts suspected of being fraudulent and associated fraud events in the National Register of Accounts Reported for Fraud Risk (FNC-RF) managed by the Banque de France, in accordance with Article L. 521-6-1 of the French Monetary and Financial Code; this registration will prompt immediate corrective filings once the reasons for suspecting fraud no longer apply; – Responding to requests from French and European authorities.

Pursuit of our legitimate interests	– Reviewing and processing job, internship, and unsolicited applications;
	– Responding to onboarding requests initiated by you and processing account-opening applications (pre-contractual measures);
	– Monitoring the quality and performance of our services;
	– Creating, testing, improving, activating, and marketing our products and services;
	– B2B sales outreach, including contacting you to introduce our banking services, enriching our sales databases, and managing our marketing campaigns;
	– Fraud prevention and detection: to protect our users, our systems, and Memo Bank against fraudulent transactions, we use internal monitoring processes and industry-shared services; these systems act solely as decision-support tools, and the final decision to block or authorize a transaction always remains subject to human review:
	  – Monitoring by our internal systems: we carry out automated processing, notably by applying our own risk assessment rules, to analyze transaction and behavioral data in order to detect anomalies and assign a risk score to a transaction;
	  – Participation in the shared FPAD (Fraud Pattern and Anomaly Detection) service: to benefit from a broader view of fraud patterns, we participate in the FPAD service operated by EBA CLEARING; we use this service to:
	  – Assess the risk level of a payee account;
	  – Assess the risk level of a transaction;
	  – Investigate previously executed transactions;
	  – Identify accounts potentially involved in fraud networks;
	  – For digital payment services (Click to Pay, Google Pay, Apple Pay), our

Legal basis	Purposes of processing
	legitimate interest lies in protecting our customers and our systems against fraud, improving transaction security by replacing the transmission of the actual card number with a tokenization system, and streamlining the checkout experience for our users. – Generating de-identified, anonymized, or aggregated datasets; – Security, technical supervision and proper functioning of our MCP server: logging of requests received and responses issued in order to detect unauthorised or abnormal access, to diagnose and remedy incidents and, where applicable, to evidence the accesses made (see Technical logging of MCP server accesses); – Recording and analyzing sales conversations (sales outreach meetings, demonstrations, follow-up meetings) held with our prospects and clients, for training and coaching purposes for our sales teams and to improve the quality of our commercial relationship; data subjects are informed of the recording prior to the interaction and may object under the conditions set out in the GDPR.
Explicit consent of the data subjects	– Retaining unsuccessful applications for future opportunities; – Direct marketing by electronic means where regulations require prior consent (opt-in); – Responding to partnership requests; – Sending newsletters and informational emails; – Responding to inquiries received on social media; – Sending invitations to webinars or physical events and tracking registrations and attendance; – Implementing programs or services offered by a company accepting card payments, by Visa, or by its partners.

For each of these purposes, we ensure that we only collect and process strictly necessary data. You have rights regarding this processing, detailed in the Right of Access, Rectification, and Erasure section of this policy.

4. How do digital payments secure your data?

Digital payment services (Click to Pay, Google Pay, Apple Pay) utilize a tokenization system to protect your banking details. During transactions, your actual card number is never shared with merchants or stored on your device. It is replaced by a unique digital token that cannot be exploited in the event of a security breach. Each transaction is secured by a single-use cryptogram.

For mobile payments, accessing the service requires your authentication (either through biometrics or your device's passcode).

5. Joint Controllership with Visa for the Click to Pay Service

For the operation of the Click to Pay service, Memo Bank and Visa act as joint controllers of your personal data, in accordance with Article 26 of the GDPR. We have defined our respective obligations to ensure the protection of your data in a dedicated agreement.

This allocation is as follows:

- Memo Bank is responsible for:
  - Collecting the personal data required to activate the service and informing you of its activation as a standard feature of your card.
  - Securely transmitting this data to Visa.
  - Managing requests regarding your rights (access, rectification, etc.), and in particular your right to opt out of the Click to Pay service (opt-out). Memo Bank is your primary point of contact for any questions regarding the use of your data in this context.
- Visa is responsible for:
  - Securely storing your information in the Click to Pay database.
  - Operating the technical infrastructure that enables you to be recognized when paying at a merchant (via your email or phone number).
  - Displaying your masked cards and transmitting the payment information necessary for the merchant to finalize the transaction, once you have selected a card.

6. Connecting Your Workspace to a Third-Party Artificial Intelligence Assistant (MCP Server)

Memo Bank provides a server compatible with the MCP (*Model Context Protocol*) which allows you, should you wish, to connect your Workspace to an artificial intelligence assistant provided by a third party (an "AI Assistant") in order to consult and make use of your banking data from within that assistant.

This feature is optional. It is activated only at your initiative, when your Representative, or a User authorised for that purpose in accordance with the services agreement, expressly authorises an AI Assistant to access your Workspace using the OAuth 2.0 secure authorisation protocol. This authorisation constitutes an express instruction to Memo Bank to transmit the relevant data to the provider of the AI Assistant, and a waiver of banking secrecy within the meaning of Article L. 511-33 of the French Monetary and Financial Code in favour of that provider and of the service providers it relies on to deliver its service, within the limits of the access scopes you have selected. The AI Assistant accesses your Workspace as an Integrator or Partner within the meaning of the services agreement: it acts, within the limits of the authorisations you have granted it, in the name and on behalf of your company, under the conditions set out in that agreement. This mandate, which governs your contractual relationships, has no bearing on the provider's qualification under the GDPR, which depends on the plan your company has subscribed to with it (see below).

6.1. Role of Memo Bank and of the AI Assistant Provider

Memo Bank acts as data controller solely for the operations it carries out: verifying your identity and your authorisation, transmitting the data you have requested, and securing and logging these accesses. This transmission is necessary to provide the feature you have requested under the services agreement between us.

Memo Bank does not determine the purposes or means of the processing carried out by the provider of the AI Assistant once the data has been transmitted, and acts neither on behalf of that provider nor jointly with it. The provider processes the data it receives under its own responsibility or, depending on the plan your company has subscribed to with it, as a processor of your company, under the conditions set out in its own terms of use and privacy policy, which we invite you to review before connecting. Memo Bank has no access to the conversations you hold with the AI Assistant or to the responses it generates; it only receives the technical requests that the AI Assistant sends to its server, which may contain the search or filtering criteria you have entered in the assistant (for example a counterparty name or a date range).

As the account holder, your company remains responsible for its choice of the AI Assistant it decides to connect and for the use it makes of the data thus obtained, including with regard to third parties (employees, customers, suppliers, counterparties) whose personal data appears in its Accounts and Payment Operations.

The notes and supporting documents you attach to your Payment Operations are data that Memo Bank processes on your behalf as a processor (see Data Processed on Behalf of Memo Bank Service Users). Their transmission to the AI Assistant is an operation that Memo Bank carries out on your documented instruction: you are the data controller for it, and the provider of the AI Assistant is a recipient designated by you, not a sub-processor of Memo Bank.

6.2. Data Transmitted

Only data falling within the access scopes (*scopes*) you have authorised is transmitted, at the request of the AI Assistant and, as of today, on a read-only basis. Depending on the scopes selected, this may include:

- information relating to your Accounts (name, IBAN, balance, currency);
- the history and details of your Payment Operations (date, amount, label, name and bank identifier of counterparties, associated notes and supporting documents);
- identification information of your company and of the Workspace users required for the connection to operate;

– technical identifiers assigned by Memo Bank to these Accounts, Operations and users, required for the connection to operate.

No login credentials (password, access code, strong authentication device) are shared with the AI Assistant. It only receives an access token limited to the scopes you have authorised, revocable at any time and of no value outside those scopes. As of today, no payment transaction can be initiated through it.

6.3. Providers Concerned and Transfers Outside the European Union

The MCP server is open: you freely choose the AI Assistant you connect, and Memo Bank neither lists nor verifies its providers. The assistant name shown on the authorisation screen and in the list of your active connections is the name declared by the assistant itself. It is your responsibility, before activating the connection, to satisfy yourself as to the identity of its provider, its country of establishment and the safeguards it offers, as described in its own privacy policy.

The AI Assistant accesses your data in your name and on your behalf, like any software you use to consult your Workspace. Where its provider is established outside the European Union, notably in the United States, the transmission of your data outside the EU/EEA results from your choice of that tool and from the contractual relationship your company has directly with its provider. It is carried out on your express instruction and under your responsibility, including for the notes and supporting documents for which you are the data controller. The safeguards framing this transfer (an adequacy decision of the European Commission, the provider's certification under the EU–US Data Privacy Framework, or Standard Contractual Clauses) are those offered by the provider within that relationship; we invite you to favour providers established in a country covered by an adequacy decision or certified under the Data Privacy Framework. The processing subsequently carried out by the provider on its own behalf or on behalf of your company falls within that same relationship. You may end this transfer at any time by revoking the connection.

6.4. Revocation

You may revoke an AI Assistant's access at any time from your Workspace settings or by contacting our customer service. Revocation ends any further transmission of data once the current access tokens are invalidated or expire. It has no effect on data already received by the provider, whose retention and erasure are governed by its own privacy policy; your rights over that data are exercised directly with it.

6.5. Technical Logging of MCP Server Accesses

In order to ensure the security of the MCP server, to detect and analyse unauthorised, abnormal or fraudulent access, to diagnose and remedy malfunctions, and to be able to account to you for the accesses made to your Workspace, Memo Bank keeps technical logs of the requests sent to its MCP server and of the responses it issues. This processing is based on the legitimate interest of Memo Bank and its customers in the security and proper functioning of the service, as well as on the security and incident-management obligations to which Memo Bank is subject as a credit institution and payment service provider.

These logs are limited to what is necessary for these purposes and comprise:

– technical events: timestamp, technical identifiers of the client, user and connection, identifier and version of the AI Assistant, requested operation and outcome (success or error), without the content of requests or responses, retained for the duration of the business relationship and then archived for five (5) years, in order to be able to evidence accesses made under a waiver of

banking secrecy during the applicable limitation period, consistently with the retention period of your banking transactions;

- the technical content of requests and responses (authorised access scopes, parameters received from the AI Assistant and banking data returned), retained for a maximum of thirty (30) rolling days and then automatically deleted. This period corresponds to the time needed to reproduce and remedy an incident reported to us and to investigate any dispute regarding an access.

These logs are encrypted, accessible only to authorised members of our technical and security teams under traceable procedures, and are used for no other purpose: they are not used for commercial or analytical purposes, nor to train artificial intelligence models, and are not shared with the provider of the AI Assistant. In the event of a security incident, a complaint or a request from an authority, the strictly necessary logs may be extracted and kept in restricted-access intermediate archiving for the duration of the handling of that event.

7. Automated Decision-Making

As part of our fraud-prevention activities, we use automated systems, including profiling, to analyze transaction and behavioral data to detect anomalies and assign a risk score to transactions.

These systems serve as decision-support tools. In accordance with Article 22 of the GDPR, no decision producing legal effects concerning you or significantly affecting you in a similar way (such as blocking a transaction) is made solely on the basis of automated processing. The final decision to block or authorize a transaction always remains a human one, involving analysis and validation by our teams.

Accesses made through our MCP server by an AI Assistant you have connected do not feed any automated decision by Memo Bank concerning you.

8. Information on the National Register of Accounts Reported for Fraud Risk (FNC-RF)

In accordance with Article L. 521-6-1 of the French Monetary and Financial Code, established by Law No. 2025-1058 of November 6, 2025, and the Order of April 24, 2026, enacted for its application, the Banque de France manages a national database known as the "FNC-RF" (Fichier National des Comptes signalés pour Risque de Fraude — National Register of Accounts Reported for Fraud Risk). This register lists information identifying payment and deposit accounts suspected of being fraudulent, alongside details characterizing the fraud or suspicion of fraud.

All payment service providers established or operating in France, including Memo Bank, are required, in the event of suspected fraud, to register the information concerning the accounts and the associated fraud events in this register. When an account of which it is the account-keeper is registered in this file, Memo Bank shall proceed, as quickly as possible, with verifications aimed at assessing its fraudulent nature. Furthermore, Memo Bank shall file corrective reports without delay as soon as new information warrants it or the reasons for suspecting fraud disappear.

The registered information is kept in the register for 13 months from the date of the declaration or the last corrective declaration.

The registration of an account in this register does not entail a prohibition on performing payment transactions involving that account, and cannot on its own justify the termination of the account agreement or the framework payment services agreement.

Memo Bank and the Banque de France are, each for its own scope, independent data controllers for the processing carried out within the framework of the FNC-RF. Your rights of access, rectification, and restriction regarding the information concerning you registered in this file must be exercised with the payment service provider that keeps your account. When Memo Bank is the keeper of your account, these rights can be exercised in accordance with the procedures described in Section Right of Access, Rectification, and Erasure of this policy. For any additional information on the operation of the FNC-RF, you may also consult the website of the Banque de France.

In accordance with Article 21 of the GDPR, the right to object does not apply to this processing, which is based on a legal obligation.

9. Recipients of Collected Data

The personal data collected is intended for the personnel authorized to process information within Memo Bank. When strictly necessary, this information may be shared with suppliers, partners, or processors, such as:

Category of recipients	Description and examples
Technical Service Providers	– Web hosting providers; – Software and productivity tool providers for our internal teams (communication tools, customer knowledge base); – Providers of specialized technology solutions (such as AI, data analytics, or cybersecurity) assisting us in the development and operation of our internal fraud-monitoring and detection tools. These providers act on our behalf and under our instructions as data processors; – Providers of conversational intelligence solutions allowing the recording, transcription, and analysis of commercial exchanges (such as Modjo), acting on our behalf and under our instructions as data processors; – Trust service providers for electronic document signatures (e.g., Yousign).

Category of recipients	Description and examples
Digital Payment Service Partners	– Visa: For the Click to Pay service, as joint controllers, we transmit the data necessary to create and manage your profile to Visa. – Mobile payment service providers: To enable Google Pay or Apple Pay, card details are encrypted on your device and transmitted securely via Google or Apple servers to validate your identity and generate the token. In accordance with their privacy policies, neither Google nor Apple stores your plain-text card number.
Market Infrastructures and Payment System Operators	– For our participation in the FPAD and VOP fraud-detection services, we transmit data to EBA CLEARING, which acts as a processor on our behalf. EBA CLEARING uses technical sub-processors (such as Nexi Payments) to operate these services' infrastructure.
Financial Service Providers	– Account Information Service Providers (AISPs); – Payment Initiation Service Providers (PISPs); – Financial institutions; – Payment and card networks; – Clearing houses; – Settlement systems; – Payment card manufacturers.

Category of recipients	Description and examples
Marketplace Partners	When you activate the connection of a third-party tool from your Workspace, you give express instructions to Memo Bank to transmit the data of your Accounts and Payment Operations to the relevant Partner, on the basis of the performance of the contract that binds us. The Partner processes the data it receives in this context under its own responsibility or, depending on the plan your company has subscribed to, as a processor of your company; its use is governed exclusively by its own privacy policy.
Third-Party Artificial Intelligence Assistant Providers (MCP Server)	When you connect an AI Assistant to your Workspace through our MCP server, you give express instructions to Memo Bank to transmit the data of your Accounts and Payment Operations to the provider of that assistant, within the limits of the access scopes you have authorised. This provider, which you freely choose, processes the data it receives under its own responsibility or, depending on the plan your company has subscribed to, as a processor of your company, under the conditions of its own privacy policy (see Connecting to an AI assistant).
Professional Service Providers	– Auditors; – Lawyers and legal counsel; – External financial advisors; – Recruitment firms.

Category of recipients	Description and examples
Regulatory Partners	– External AML/CFT service providers; – Supervisory authorities; – Judicial authorities, law enforcement, or competent public bodies (such as TRACFIN in France) when we are required to file a suspicious transaction report or respond to a legal warrant; – The Banque de France, in its capacity as manager of the national database of accounts reported for fraud risk (FNC-RF) under Article L. 521-6-1 of the French Monetary and Financial Code; – Administrative and public authorities.
Guarantor Organizations	– In the framework of financing operations benefiting from a guarantee, the guarantor organization as well as any party it mandates may access, for control and verification purposes, the documents and data relating to the operations concerned, during the applicable retention period.
Authorized Users	– Account holders, to whom the data relating to the use of the Workspace and the actions performed by the users of the account opened in the books of Memo Bank may be addressed.

Moreover, data relating to the use of the Workspace and the actions performed by the users of the account opened in the books of Memo Bank may be transmitted to the account holder.

Personal data collected by Memo Bank on the Site for sales prospecting or communication is strictly for internal use and will not be sold or shared for commercial purposes.

10. Data Retention Periods

Memo Bank retains your personal data only for as long as necessary to fulfill the purposes for which it was collected. Retention periods vary depending on the nature of the data and the processing purposes. At the end of these periods, certain data may undergo intermediate archiving for legal or litigation reasons before being permanently deleted.

By way of example, the main retention periods we apply are as follows:

Data category	Retention period
Identification data (KYC/KYB) and data linked to AML/CFT	5 years from the end of the business relationship.
Banking transactions and movements	5 years from the end of the business relationship.
Data processed within the framework of loan agreements and guarantee deeds	5 years from full repayment of the credit or the discharge of the guarantor's commitment.
Documents relating to financing operations benefiting from a guarantee	10 years from the loan disbursement date, in accordance with the obligations undertaken with the guarantor.
Documents and supporting evidence related to operations	10 years (legal accounting retention).
Commercial prospecting data	3 years from the last active contact.
Recordings of commercial conversations and associated metadata	3 years from the recording date, aligned with the retention period for commercial prospecting data.
Data on unsuccessful applications	2 years from the last contact.
Service usage data — application and security logs	1 year, then intermediate archiving for 2 years (3 years in total), from collection.
Service usage data — browsing data and cookies	13 months from the placement of the cookie or tracker.
Event logs and register of ICT providers (DORA)	5 years.
Card transaction data, including payments made via Click to Pay	13 months from the debit date; accounting archive of up to 10 years (Article L. 123-22 of the French Commercial Code).
Click to Pay profile data hosted by Visa	Retained by Visa for the periods defined in its own privacy policy, under its responsibility.
Data processed in connection with the Verification of Payee (VOP) service	Raw queries: 8 days. Associated transaction data: 14 months. Security audit logs: 10 years.
Data processed in connection with the FPAD fraud-detection service	Transactions and API queries: 14 rolling months. Aggregated fraud reports: 8 calendar days. Model version history: 14 rolling months. Anonymised transaction data used for training: 3 years maximum.
Data transmitted to Marketplace Partners	This data is retained for the durations defined by each Partner in their own privacy policy, under their sole responsibility as independent data controllers.

Data category	Retention period
Data transmitted to an AI Assistant provider through the MCP server	This data is retained for the durations defined by the provider concerned in its own privacy policy, under its responsibility.
MCP server technical logs — content of requests and responses	30 rolling days, automatic deletion (see Technical logging of MCP server accesses).
MCP server technical logs — technical events (identifiers only)	Duration of the business relationship, then 5 years.
Technical identifiers assigned to your Accounts, Payment Operations and users	Retention period of the data to which they relate.
Data reported to the FNC-RF register	13 months from the filing date or the most recent corrective update, in accordance with Article 6 of the Order of April 24, 2026.

11. Right of Access, Rectification, and Erasure

In accordance with applicable regulations, users have the following rights:

Right	Description
Right of access	The right to obtain information about how your personal data is processed, as well as a copy of that data.
Right to rectification	If you believe your personal data is inaccurate or incomplete, the right to request that it be corrected or updated accordingly.
Right to erasure	The right to demand the deletion of your personal data, within the limits of applicable regulations.
Right to restriction of processing	The right to request that the processing of your personal data be restricted.

Right	Description
Right to object	The right to object to the processing of your personal data on grounds relating to your particular situation. You have an absolute right to object to the processing of your personal data for direct marketing purposes, including profiling related to such marketing. Concerning specifically the Click to Pay service, you have the right to unsubscribe (opt-out) at any time. Since this service is activated by default to facilitate your payments, you can request its deactivation simply and at any time from your Workspace or by contacting our customer service. This deactivation will have no impact on the other features of your card.
Right to portability	Where applicable, the right to have the personal data you provided to Memo Bank returned to you or, where technically feasible, transmitted directly to a third party.
Right to withdraw consent	If you have given consent to the processing of your personal data, the right to withdraw that consent at any time.

These rights may be exercised by submitting a written request via email (see our contact page). Where there is reasonable doubt as to the identity of the requester, we may ask for proof of identity. All requests must be clear and specific.

For data transmitted to a Marketplace Partner, these rights must be exercised directly with the Partner, acting as an independent data controller for such data.

For data transmitted to an AI Assistant through our MCP server, these rights are exercised directly with the provider concerned for the processing it carries out, and with Memo Bank for the technical logs it retains.

12. Security

We process personal data in a manner that ensures appropriate security using physical, technical, and organizational measures that align with state-of-the-art standards. This includes protection against unauthorized or unlawful processing, as well as accidental loss, destruction, or damage. In accordance with our obligations, Data Protection Impact Assessments (DPIAs) have been conducted for processing operations presenting a high risk to the rights and freedoms of individuals.

To ensure the security of your data, we implement the following measures in particular:

Measure	Description
Resilience and business continuity	Our banking system is designed to be resilient and scalable, thus ensuring a high level of business continuity in the event of an incident.
Four-eyes validation	Each modification or intervention on our core banking system is verified and validated by a third party, thereby limiting the risks of error.
Incident management	We have set up a rigorous incident management procedure, including a proactive qualification of events and the writing of analysis reports for major incidents.
Data encryption	We systematically encrypt sensitive banking data, including when stored on our employees' workstations. We also use data pseudonymization as appropriate, depending on the needs, risks, and purpose of the processing.
Firewalls	We use firewalls to protect our systems against unauthorized access.
Antivirus	Our systems are protected by regularly updated antivirus software.
Multi-factor authentication	We use multi-factor authentication to strengthen the security of access to our systems and your accounts.
Access control	Access to your data is strictly limited to authorized personnel who require it to perform their duties.
System monitoring	Our systems are constantly monitored to detect any suspicious activity.
Employee training	Our employees regularly complete mandatory training in personal data protection and cybersecurity.
Security tests and analyses	We regularly test, analyze, and evaluate the effectiveness of our security measures.
External experts	We regularly call upon external experts to analyze the robustness of our systems and their compliance with security requirements, in particular those required by Swift from credit institutions.

In any case, persons likely to process personal data within Memo Bank are subject to a strict obligation of confidentiality and to banking secrecy, the violation of which is punishable both criminally and civilly.

13. Data Hosting

Our servers, on which the Site is notably hosted, are located in the data centers of Google Cloud Platform and Amazon Web Services within the European Union.

14. Data Transfers Outside the European Union

Some of your personal data may be transferred outside the European Union (EU) or the European Economic Area (EEA) when we engage certain service providers. This notably applies to:

- The use of customer relationship management software like HubSpot or support software like Help Scout, whose servers are located in the United States.
- The use of digital payment services like Click to Pay (operated by Visa), Google Pay, or Apple Pay, which involve data transfers to the United States to operate these services.
- The activation, at your initiative, of a Marketplace Partner established outside the EU/EEA: this transfer is made on your express instruction, to Partners established in a country covered by an adequacy decision or certified under the *Data Privacy Framework*; the Partner's subsequent processing is governed by its own privacy policy.
- The connection, at your initiative, of an AI Assistant whose provider is established outside the EU/EEA through our MCP server: this transfer results from your choice of that tool and is made on your express instruction and under your responsibility, under the conditions described in Section Connecting to an AI assistant.

We ensure that each transfer of data outside the EU/EEA is framed by appropriate safeguards, in accordance with the GDPR. These safeguards rely first and foremost on adequacy decisions of the European Commission, in particular the EU–US Data Privacy Framework under which our main providers established in the United States are certified, and, as a complement, on the signing of Standard Contractual Clauses (SCCs) approved by the European Commission, thus ensuring an adequate level of protection for your data in compliance with European law.

15. Personal Data Processed by Memo Bank as a Data Processor

In certain instances, Memo Bank acts as a personal data processor. This means we process personal data on behalf of and under the instructions of another organization, which acts as the data controller.

15.1. Data Processed on Behalf of Memo Bank Service Users

In order to fulfill our obligations under the services agreement, we are likely to process personal data in the name and on behalf of the users of our services when they decide to save documents containing personal data concerning third parties in their Workspaces.

This may notably concern supporting documents attached to payment operations (such as invoices, contracts, purchase orders) from which they may ask us to extract this data in a digital format using an optical character recognition (OCR) tool; personalized notes they add to operations; or direct debit mandates signed electronically with their debtors.

In these scenarios, the user acts as the data controller within the meaning of the regulations, as they determine the purposes and means of the processing, and we act as a data processor, processing the data solely on the user's instructions.

For their part, users undertake to comply with applicable regulations and to instruct us to process only data that is relevant, proportionate, and necessary for the described processing operations.

This personal data is used by us, upon instruction of the user, in order to manage their expenses and collections, as well as to manage the supporting documents of expenses and perform accounting reconciliation.

The personal data we may process as a processor on behalf of our users notably includes:

- data relating to civil status, such as the name, first name, email address, or phone number of third parties;
- data of a banking and financial nature concerning third parties, such as account or payment card numbers;
- data relating to the professional life of third parties, such as the position held by the persons whose personal data is processed by the users.

Our commitments as a processor for the user:

- we process the data only on documented instructions from the user;
- we apply to this sub-processed personal data the same technical and organizational security measures as those we apply in our capacity as a data controller and which are described in the relevant section of this policy, the persons authorized to process this data being subject to an obligation of confidentiality;
- any possible transfer of sub-processed personal data on behalf of users must obey the requirements we apply in our capacity as a data controller and which are described in the relevant section of this policy (Data Transfers Outside the European Union);
- in the event of a personal data breach affecting the data processed on behalf of a user, we undertake to notify the user concerned as quickly as possible, and at the latest within 72 hours after having become aware of it, and to communicate to them all useful information required by the regulations;
- during the entire duration of the contractual relationship with the users, we undertake to respond as quickly as possible to any request to exercise a right transmitted by the user (concerning the data of the third parties they control) or to provide all the information necessary in the framework of a data protection impact assessment (DPIA) or a request from the authorities; in this respect, we keep in writing a register of all categories of processing activities carried out on behalf of our data controller users.

To host this data, we engage the following sub-processors: Google Cloud Platform and Amazon Web Services, whose servers are located within the European Union.

The transmission of this data, on your instruction, to an AI Assistant you have connected through our MCP server (see Connecting to an AI assistant) does not constitute the engagement of a sub-processor by Memo Bank: the provider of the AI Assistant is a recipient designated by you and for which you are answerable.

Should we engage other sub-processors for these operations, we will inform our users in advance in writing by updating this Privacy Policy.

In accordance with regulations, users may submit reasoned objections to such changes.

In the absence of such objections within a period of fifteen days from this information, we consider that our user has accepted the changes to the list of subsequent sub-processors.

Any subsequent sub-processor is bound to respect the same contractual and regulatory obligations as ours, in particular regarding security and personal data transfers, and we remain fully liable to our users for the execution by the subsequent sub-processor of its obligations.

In accordance with the regulations, we make available to our data controller users all the information necessary to demonstrate compliance with the obligations provided for in this section.

15.2. Data Processed on Behalf of Twenty First Capital

In the framework of the provision of the Investment Services, as defined in the General Terms and Conditions, we also act as a personal data processor on behalf of the company Twenty First Capital when we act in our capacity as a tied agent of this investment services provider.

In this context, Twenty First Capital acts as a data controller, determining the purposes and essential means of the processing. Memo Bank acts as a processor, processing the data on the documented instructions of and on behalf of Twenty First Capital.

The processing that Memo Bank carries out on behalf of Twenty First Capital is necessary in order to enable our customers to subscribe to the Investment Services of Twenty First Capital.

In accordance with Twenty First Capital's instructions, within the framework of the provision of these Investment Services, the personal data we may process on behalf of Twenty First Capital includes:

- identification data of our customers (and/or the natural persons who are linked to them when they are legal entities) who subscribe to the Investment Services of Twenty First Capital; this may include the names, first names, dates of birth, and copies of identity documents of the natural persons concerned (such as, for legal entities, their legal representatives, ultimate beneficial owners, or employees administering the account);
- connection data, such as IP addresses and connection logs linked to the use of the Investment Services concerned.

The categories of data subjects for this specific processing are therefore our customers (and the natural persons who are linked to them) who subscribe to the Investment Services of Twenty First Capital.

Our commitments as a processor for Twenty First Capital:

- we process this personal data only on documented instructions from Twenty First Capital and inform Twenty First Capital if an instruction constitutes, in our opinion, a violation of applicable law;
- we are responsible for the security of the personal data entrusted to us on behalf of Twenty First Capital and take all appropriate technical and organizational measures in order to guarantee a level of security adapted to the risk; these measures are analogous to those described in the relevant section of this policy (Security);
- we ensure that the persons authorized to process the personal data have knowledge of the instructions of Twenty First Capital and are subject to an appropriate obligation of confidentiality;
- we undertake not to transfer the personal data outside the European Economic Area or countries recognized as having an adequate level of protection by the European Commission without informing Twenty First Capital beforehand and without the implementation of appropriate safeguards within the meaning of the GDPR; these safeguards may be similar to those described in the relevant section of this policy (Data Transfers Outside the European Union); if we are required to proceed with such a transfer under applicable law, we will inform Twenty First Capital of this

legal requirement beforehand, unless this law prohibits us from doing so for important reasons of public interest;

- we inform Twenty First Capital as quickly as possible of any personal data breach of which we have knowledge and which would affect the data processed on its behalf; we undertake to use our best efforts to assist Twenty First Capital in fulfilling its own obligations; this includes assistance in responding to requests from data subjects to exercise their rights (by communicating to it any request we may receive), as well as collaboration in the framework of impact assessments or formalities with the CNIL.

For the execution of the Investment Services on behalf of Twenty First Capital, and with its express notification and acceptance, we call upon the following subsequent sub-processors: Google Cloud Platform, Amazon Web Services, and Jotform.

Twenty First Capital is informed of any addition or replacement within this list, giving it the possibility to issue reasoned objections.

We impose on these subsequent sub-processors the same data protection obligations as those incumbent on us, and we remain fully liable to Twenty First Capital for the compliance with these obligations by the subsequent sub-processors.

Concerning the data processing carried out within the framework of the Investment Services for which Twenty First Capital is the data controller, in order to exercise their rights (access, rectification, erasure, objection, restriction, portability), data subjects are invited to contact Twenty First Capital in the first instance. If we receive a request to exercise rights concerning this processing, we will forward it to Twenty First Capital as quickly as possible.

16. Cookie Management

We use cookies on our website to improve your user experience and analyze traffic. For more information on the types of cookies we use and how to manage them, we invite you to read our cookie management policy.

17. Amendments

We reserve the right to modify this Privacy Policy. In the event of a substantial modification, you will be informed by any appropriate means, in particular by email or by a notification in your Workspace. The date of the last update is indicated at the head of this document.

18. Complaints

For any question concerning the Privacy Policy, the user must make their request by email (see our contact page) or contact our Data Protection Officer at protectiondesdonnees@memo.bank.

They also have, regarding the processing of personal data, the possibility of lodging a complaint with the Commission Nationale de l'Informatique et des Libertés (CNIL), the supervisory authority for personal data. To refer a matter to the CNIL, one should either carry out the process online by visiting the site cnil.fr, or send a letter to the attention of the president of the CNIL, Commission Nationale de l'Informatique et des Libertés – 3, Place de Fontenoy – TSA 80715 – 75334 Paris Cedex 07, France.

Any request must be clear and precise and made in accordance with the applicable legal framework.