

Data Processing Agreement (DPA)

Version 1, effective 17 August 2026

Junga SAS — <https://www.junga.ai/en/dpa>

This data processing agreement governs the processing of personal data that Junga carries out on behalf of the wealth-management advisory firms using its platform. It is entered into between the following parties.

JUNGA, a société par actions simplifiée registered with the Lyon trade and companies register under number 106 948 045, whose registered office is at Bureau 3, 30 avenue Maréchal Foch, 69006 Lyon, France, hereinafter "Junga", acting as processor.

The firm identified in the services contract entered into with Junga, hereinafter the "Firm", acting as controller.

Hereinafter referred to collectively as the "Parties" and individually as a "Party". This agreement is hereinafter referred to as the "Agreement".

1. Purpose and relationship with the services contract

1.1. Purpose

The Agreement sets out the conditions under which Junga processes, as processor, the personal data for which the Firm is the controller, in accordance with Article 28 of Regulation (EU) 2016/679 (hereinafter the "GDPR") and with French Act no. 78-17 of 6 January 1978, as amended.

It applies to all processing carried out by Junga on behalf of the Firm within the platform, whatever the module used and the access channel, including the white-label client portal made available to the Firm's end clients.

1.2. Relationship with the services contract

The Agreement supplements the services contract entered into between the Parties and forms an integral part of it. It does not replace it: the provisions relating to price, term, service levels and the practical performance of the services remain governed by that contract.

Acceptance of the services contract constitutes acceptance of the Agreement. Firms that require a signed copy may request one at dpo@junga.ai.

1.3. Order of precedence

In the event of a conflict between the Agreement and the services contract on a matter relating to the processing of personal data, the Agreement prevails. On any other matter, the services contract prevails.

No provision of the Agreement may be construed as relieving either Party of an obligation that applies to it directly under the applicable data protection legislation.

2. Roles of the Parties and definitions

2.1. Definitions

The terms "personal data", "processing", "controller", "processor", "data subject", "personal data breach" and "supervisory authority" have the meaning given to them by Article 4 of the GDPR. The following terms are specific to the Agreement.

- End clients: the natural persons whose wealth relationship the Firm manages and whose data is processed in the platform, together with the beneficial owners identified by the Firm.
- Firm Users: the Firm's staff holding an account on the Junga dashboard.
- Platform: the dashboard intended for the Firm, the white-label client portal and the associated application interfaces.
- Sub-processor: any third party to which Junga entrusts all or part of a processing operation carried out on behalf of the Firm.

2.2. The Firm, as controller

The Firm determines the purposes and means of the processing of its end clients' data. It is responsible for ensuring that a legal basis exists for each processing operation, that the data it transmits to Junga is lawful, accurate and up to date, and that it complies with the obligations applicable to it under the legislation governing its business.

2.3. Junga, as processor

Junga processes end clients' data solely on behalf of the Firm and on its documented instructions, under the conditions described in the Agreement.

Junga remains the controller for the data it processes on its own behalf, in particular Firm Users' accounts, subscription billing and platform security. That processing is described in the privacy policy published at www.junga.ai and does not fall within the scope of the Agreement.

2.4. Informing data subjects

It is for the Firm to inform its end clients of the processing of their data, in accordance with Articles 13 and 14 of the GDPR. Junga provides it with a template information notice for the client portal. That template is provided as an aid and does not constitute legal advice: the Firm remains responsible for the information actually given to its end clients.

3. Description of the processing carried out on behalf of the Firm

This section describes, in accordance with Article 28(3) of the GDPR, the subject matter, nature, purpose and duration of the processing carried out on behalf of the Firm, together with the categories of data and of data subjects. It is taken from the record of processing activities maintained by Junga under Article 30(2) of the GDPR.

3.1. Nature and purposes of the processing

Junga carries out the following processing on behalf of the Firm.

- Client management (KYC and onboarding): building and maintaining the regulatory client file on behalf of the Firm.
- Identity verification (KYC documents): checking identity documents and detecting document fraud.
- MiFID II suitability questionnaire: assessing product suitability (investor profile).
- AML-CFT screening (asset freezes, politically exposed persons, sanctions): detecting persons subject to sanctions or who are politically exposed.
- Wealth management (assets and valuations): tracking assets and their valuations for wealth advice.
- White-label client portal: a client area in the Firm's colours (documents, signature, simulators).
- Transactional emails: service notifications (invitations, document reminders, signatures).
- Electronic signatures: signing of regulatory documents (entry-into-relationship document, engagement letters).

The operations carried out on this data are collection, recording, organisation, structuring, storage, consultation, use, matching, making available to the Firm and its end clients, restriction and erasure.

3.2. Categories of personal data

- Client management (KYC and onboarding): identity, contact details, family situation, wealth data.
- Identity verification: identity documents and data resulting from facial matching.
- MiFID II suitability questionnaire: financial situation, objectives, financial knowledge.
- AML-CFT screening: identity, politically-exposed-person status, data relating to criminal convictions and offences.
- Wealth management: financial assets, bank accounts obtained through aggregation, valuations.
- White-label client portal: identity, authentication data, documents.
- Transactional emails: email address, name, content of the notifications.
- Electronic signatures: identity, email address, signature evidence.

3.3. Data subject to a specific regime

Two processing operations may involve data subject to a specific regime.

Identity verification may include facial matching, which constitutes processing of biometric data for the purpose of uniquely identifying a natural person within the meaning of Article 9 of the GDPR. That processing is carried out on behalf of the Firm, under its obligations to verify the identity of its clients. The Firm, as controller, ensures that a condition for lawfulness laid down in Article 9(2) is met; Junga and its identity-verification sub-processor assist it to that end, in particular by obtaining the person's explicit consent within the verification journey where that basis is relied on.

AML-CFT screening may reveal data relating to criminal convictions and offences within the meaning of Article 10 of the GDPR. That processing is carried out in order to meet the Firm's legal obligations and access to this data is strictly limited.

3.4. Categories of data subjects

- The Firm's end clients.
- The beneficial owners identified in the course of AML-CFT screening.
- Firm Users, for the transactional emails addressed to them.

3.5. Duration of the processing and retention periods

The processing is carried out throughout the term of the services contract. The retention periods applied in the platform, determined by the legal obligations that apply to the Firm, are as follows.

- Client management (KYC and onboarding): five years after the end of the business relationship (Article L.561-12 of the French Monetary and Financial Code), followed by five years of archiving.
- Identity verification: five years after the end of the business relationship.
- MiFID II suitability questionnaire: five years, the questionnaire being renewed every two years.
- AML-CFT screening: five years, in a tamper-proof log.
- Wealth management: the duration of the relationship, then five years; valuations are kept as a tamper-proof history.
- White-label client portal: the duration of the relationship; authentication sessions are kept for one year.
- Transactional emails: logs kept for one year; deletion of the logs held by the sending provider within thirty days.
- Electronic signatures: ten years (eIDAS Regulation and Article 1366 of the French Civil Code).

The platform's audit logs are kept for five years and can be neither modified nor deleted, in order to guarantee traceability that can be relied on during an inspection.

4. Documented instructions

Junga processes the Firm's data only on the Firm's documented instructions, including with regard to transfers of data to a third country or to an international organisation.

The following constitute documented instructions of the Firm: the Agreement and the services contract, the use of the platform by Firm Users, the configuration chosen by the Firm (settings for KYC, the MiFID II questionnaire, the AML-CFT framework, the client portal and the document templates), and any request made in writing by an authorised person of the Firm.

Any additional or derogating instruction is issued in writing. Where carrying it out entails additional development work or costs, the Parties agree on them beforehand.

Junga informs the Firm without delay if it considers that an instruction infringes the GDPR or another provision of Union or Member State law relating to data protection. Junga may suspend performance of that instruction until the Firm confirms, amends or withdraws it.

Where Junga is required to process data under Union law or French law, it informs the Firm before carrying out the processing, unless that law prohibits such information on important grounds of public interest.

5. Confidentiality of authorised persons

Junga ensures that the persons authorised to process the Firm's data undertake to keep it confidential or are subject to an appropriate statutory obligation of confidentiality.

That undertaking arises from the employment contract for employees and from a confidentiality agreement for contractors. It survives the end of the relationship between Junga and the person concerned.

Access to the Firm's data is limited to the persons who need it to perform the services, to the extent necessary for their duties. Access rights are individual and logged.

6. Security of the processing

Junga implements appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in accordance with Article 32 of the GDPR. Those measures are as follows.

- Hosting of the data in the European Union, in the Paris region of Amazon Web Services.
- Encryption of data in transit using TLS and at rest using the Amazon Web Services key management service.
- Partitioning of data between firms: each firm accesses only its own data, this partitioning being continuously verified by blocking automated tests built into the integration pipeline.
- Separation of the authentication spaces of the dashboard and of the client portal, so that a session opened on the portal can under no circumstances give access to the dashboard.

- Authenticated, role-based access control, with two-factor authentication and passkeys available for Firm Users' accounts.
- Logging of sensitive actions in an audit log that can be neither modified nor deleted, kept for five years.
- Storage of supporting documents and files in an encrypted object storage space, with no possible execution of uploaded files and with version retention.
- Continuous monitoring of availability and of application errors, personal data being masked before transmission to the monitoring service.
- Automated database backups allowing point-in-time restoration.
- Review and evolution of these measures in light of the state of the art, the risks identified and changes to the platform.

7. Sub-processors

7.1. General authorisation

The Firm gives Junga general authorisation to engage sub-processors for the performance of the services, under the conditions laid down in Article 28(2) and (4) of the GDPR.

Junga imposes on each sub-processor, by contract, data protection obligations equivalent to those of the Agreement. Junga remains fully liable to the Firm for the sub-processor's performance of its obligations.

7.2. List of sub-processors

The list of sub-processors, stating the service provided, the location of the processing and the applicable transfer safeguard, is set out in Annex 1 to the Agreement, of which it forms an integral part. It is not published: Junga makes it available to the Firm in its Billing > Platform Agreement area and provides it, on request sent to dpo@junga.ai, to any person considering entering into the services contract.

7.3. Change of sub-processor

Junga informs the Firm of any plan to add or replace a sub-processor, by updating Annex 1 and by a notification sent to the Firm, at least thirty days before the new sub-processor starts processing data on behalf of the Firm.

By way of exception, where the replacement is made necessary by a security or service-continuity imperative, in particular in the event of an incident affecting a sub-processor or the sudden discontinuation of its service, Junga may proceed without notice. It then informs the Firm without undue delay, and at the latest five business days after go-live. In that case the Firm has fifteen days from the notification to exercise the right to object set out below.

The Firm may object to that change on legitimate data protection grounds, by notifying Junga in writing before that period expires. The Parties then seek a reasonable solution. Failing agreement, the Firm may terminate the services contract for the part of the services concerned, with no indemnity on either side.

7.4. Transfers outside the European Union

The data is hosted in the European Union. Some sub-processors are established outside the European Economic Area, in the United States and in Canada; Annex 1 identifies them.

These transfers are governed by the standard contractual clauses adopted by the European Commission, supplemented where appropriate by additional measures. Junga documents the mechanism applicable to each provider in its vendor register and provides the Firm, on request sent to dpo@junga.ai, with a copy of the applicable safeguards.

Junga does not transfer any of the Firm's data to a third country outside these cases without the Firm's prior instruction.

8. Assistance to the Firm

8.1. Data subject rights

Junga assists the Firm, by appropriate technical and organisational measures and insofar as possible, in fulfilling requests to exercise the rights laid down in Chapter III of the GDPR: access, rectification, erasure, restriction, portability and objection.

Where a request to exercise rights is sent directly to Junga by an end client of the Firm, Junga does not answer it on the merits. It forwards the request to the Firm without undue delay and informs the data subject that they must contact their adviser.

Assistance is provided through the platform's features and, failing that, through ad hoc action by Junga's teams.

8.2. Security, impact assessments and prior consultation

Taking into account the nature of the processing and the information available to it, Junga assists the Firm in ensuring compliance with the obligations laid down in Articles 32 to 36 of the GDPR, in particular the security of processing, the notification of breaches, the carrying out of data protection impact assessments and prior consultation of the supervisory authority.

Junga provides the Firm, on request, with the information necessary for that work in respect of the part of the processing it operates.

8.3. Personal data breaches

Junga notifies the Firm of any personal data breach affecting the data processed on its behalf, without undue delay and at the latest 48 hours after becoming aware of it.

The notification describes, to the extent of the information available at the time it is sent: the nature of the breach, the categories and approximate number of data subjects and of records concerned, the likely consequences, the measures taken or proposed to address the breach and mitigate its effects, and the contact details of the point of contact. Missing information is provided as it becomes available, without further undue delay.

It is for the Firm, as controller, to assess the breach and, where applicable, to notify it to the Commission nationale de l'informatique et des libertés within the seventy-two-hour period laid down in Article 33 of the GDPR and to inform the data subjects. Junga makes those notifications neither in place of the Firm nor on its behalf, save on the Firm's written instruction.

Junga documents the breaches of which it becomes aware and cooperates with the Firm in producing the documentation for which the Firm is responsible.

9. Audit and demonstration of compliance

Junga makes available to the Firm all the information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR, in accordance with point (h) of paragraph 3 thereof.

The Firm may have an audit carried out, including an inspection, by itself or by an independent auditor it appoints and which is not a competitor of Junga. The audit takes place on reasonable written notice, during business hours, without excessive disruption to Junga's activity and subject to a confidentiality undertaking by the auditor.

The audit may cover only the processing carried out on behalf of the Firm. It gives access neither to other firms' data, nor to third parties' personal data, nor to elements the disclosure of which would compromise the security of the platform or Junga's confidentiality undertakings towards its other clients.

Junga may satisfy an audit request by providing existing documentation: a description of the technical and organisational measures, the results of internal controls, answers to a security questionnaire and, once they exist, audit reports or certificates issued by an independent third party.

Except where the audit follows a data breach affecting the Firm or reveals a failure by Junga to comply with the Agreement, the costs of the audit are borne by the Firm, including the time Junga spends on it, charged at the rate agreed between the Parties. Save in exceptional circumstances, on-site audits are limited to one per calendar year.

10. Fate of the data at the end of the services

On expiry or termination of the services contract, the Firm chooses between the return of the data processed on its behalf and its deletion. It expresses that choice in writing.

In the event of return, Junga makes available to the Firm an export of the data in a structured and commonly used format, together with the documents stored in the platform.

Junga then deletes the data from its active systems and has the copies held by its sub-processors deleted, within a period agreed between the Parties. Data present in backups is deleted upon expiry of the backup retention cycle.

By way of exception, Junga retains the data whose retention is required by Union law or by French law, in particular records relating to the fight against money laundering and terrorist financing (five years after the end of the business relationship, Article L.561-12 of the French Monetary and Financial Code), electronically signed documents (ten years) and audit logs (five years). The processing of that data is then limited to its storage and to the purpose that requires it, until the applicable period expires.

Junga confirms to the Firm in writing that the return and deletion operations have been carried out.

11. Term, liability and governing law

11.1. Term

The Agreement enters into force on the effective date of the services contract and remains applicable for as long as Junga processes personal data on behalf of the Firm. The provisions which, by their nature, are intended to survive it, in particular those relating to confidentiality and to the fate of the data, remain applicable after it ends.

11.2. Liability

Each Party is liable for the damage caused by processing which infringes the GDPR, under the conditions laid down in Article 82 thereof. Junga is liable for the damage caused by processing only where it has not complied with the obligations specifically directed to processors or where it has acted outside or contrary to the lawful instructions of the Firm.

The limitations and caps on liability set out in the services contract apply to the Agreement, to the extent permitted by law.

11.3. Governing law and jurisdiction

The Agreement is governed by French law. Any dispute concerning its validity, interpretation or performance falls within the jurisdiction designated by the services contract.

11.4. Contact

Any request relating to the Agreement is to be sent to Junga's Data Protection Officer, Nicolas Molins, at dpo@junga.ai or by post to the registered office.