MONESA

Data Processing Agreement

Template — to be completed and signed by the Controller (Customer) and the Processor (Monesa). Aligned with Article 28 GDPR and the EU Standard Contractual Clauses where applicable.

Controller (Customer)	Processor
Legal name: _____ Company no.: _____ Address: _____ Representative: _____ Email: _____	Monesa AB Company no.: [to be filled] Address: [to be filled], Sweden Representative: Data Protection Officer Email: privacy@monesa.ai

1. Subject matter and duration

This DPA governs the Processor's processing of personal data on behalf of the Controller in connection with the Monesa AI Investment Overview platform (the "Service"). It is effective from the date of last signature and remains in force for as long as the Processor processes personal data on behalf of the Controller.

2. Nature and purpose of processing

The Processor processes personal data to provide, secure, support and improve the Service, including hosting, authentication, audit logging, analytics, and customer support.

3. Categories of data subjects

Employees, contractors and other authorized users of the Controller, as well as individuals referenced in content the Controller uploads to the Service.

4. Categories of personal data

Identification data (name, email, job title, department); authentication data; usage and log data (IP address, device, actions performed); and any personal data contained in customer content stored in the Service.

5. Obligations of the Processor

The Processor shall: (a) process personal data only on documented instructions from the Controller, including this DPA and the Service configuration; (b) ensure that persons authorized to process personal data are under an appropriate obligation of confidentiality; (c) implement the technical and organizational measures set out in Annex II; (d) assist the Controller in fulfilling its obligations under Articles 32–36 GDPR; (e) at the Controller's choice, delete or return all personal data at the end of the engagement.

6. Sub-processors

The Controller provides general authorization for the Processor to engage sub-processors. The current list is set out in Annex III and available at https://monesa.ai/security. The Processor will notify the Controller of intended changes at least 30 days in advance and the Controller may object on reasonable grounds related to data protection.

7. International transfers

All production data is stored within the European Union. Where transfers outside the EU/EEA are necessary, they will be based on the European Commission's Standard Contractual Clauses (Module 2 or 3, as applicable) and supplementary measures where required.

8. Security

The Processor implements the technical and organizational measures described in Annex II, including encryption in transit and at rest, role-based access control, audit logging, vulnerability management and incident response.

9. Personal data breach

The Processor shall notify the Controller without undue delay, and in any event within 72 hours of becoming aware of a personal data breach, providing the information required under Article 33(3) GDPR.

10. Data subject rights

The Processor shall, taking into account the nature of the processing, assist the Controller by appropriate technical and organizational measures in fulfilling the Controller's obligation to respond to requests from data subjects under Chapter III GDPR. In-product self-service for access (Art. 20) and deletion (Art. 17) is available under Settings → My data & privacy.

11. Audits

The Processor shall make available to the Controller all information necessary to demonstrate compliance with Article 28 GDPR and allow for and contribute to audits, including inspections, conducted by the Controller or an auditor mandated by the Controller. The Processor may satisfy this obligation by providing relevant third-party audit reports or security questionnaire responses (e.g. CAIQ-Lite).

12. Liability and governing law

Liability under this DPA is governed by the master agreement between the parties. This DPA is governed by the laws of Sweden, without regard to its conflict-of-laws principles.

Annex I — Description of processing

As described in sections 2–4 above. Frequency: continuous, for the duration of the Service.

Annex II — Technical and organizational measures

• Encryption in transit (TLS 1.2+) and at rest (AES-256).

• Role-based access control with least-privilege engineering access; MFA enforced for production access.

• Row-Level Security in the database enforces per-organization data isolation.

• Append-only audit log of security-relevant events; CSV export available to company admins.

• Daily encrypted backups with point-in-time recovery; backups retained for up to 35 days.

• Vulnerability management: dependency scanning on every build, security patches within agreed SLAs.

• Input validation on all server endpoints; webhook signatures verified with constant-time comparison.

• Documented incident response process with on-call rotation and defined severity levels.

• Personnel security: confidentiality undertakings, security training, background checks where lawful.

• Sub-processor DPAs in place; sub-processors restricted to providers with equivalent safeguards.

Annex III — Sub-processors

The current list of sub-processors (hosting, authentication, email delivery, AI inference) is published at https://monesa.ai/security and is provided as a separate annex on request to privacy@monesa.ai.

Signatures

For the Controller	For the Processor (Monesa)
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____
Signature: _____	Signature: _____