

RONDANINI FX RISK INTELLIGENCE

Enterprise Data Processing Addendum

Version 1.1 — 15 September 2026

Use only where FXRI processes personal data on the Customer's behalf as processor.

IMPORTANT: This DPA does not automatically apply to ordinary account administration, billing, authentication, security, service analytics or contract evidence where the Supplier acts as an independent controller. It applies only to processing expressly identified as processor processing in Schedule 1 or another written Order.

Parties and Status

This Data Processing Addendum (DPA) forms part of the contract between {{SUPPLIER_LEGAL_NAME}} (Supplier) and {{CUSTOMER_LEGAL_NAME}} (Customer) for Rondanini FX Risk Intelligence. It applies only to the extent the Supplier processes Customer Personal Data on behalf of the Customer as a processor.

For processing covered by this DPA, the Customer is the controller and the Supplier is the processor unless Schedule 1 states otherwise. If the parties' actual roles differ under applicable law, their legal status is determined by the facts and applicable law, not merely by labels used in this DPA.

1. Definitions

Applicable Data Protection Law: the UK GDPR, Data Protection Act 2018 and other data-protection law applicable to the Processing.

Customer Personal Data: Personal Data processed by the Supplier on behalf of the Customer under the Contract and identified in Schedule 1.

Data Subject: has the meaning given by Applicable Data Protection Law.

Personal Data: has the meaning given by Applicable Data Protection Law.

Processing: has the meaning given by Applicable Data Protection Law.

Restricted Transfer: a transfer of Personal Data that requires an approved transfer mechanism under Applicable Data Protection Law.

Subprocessor: a processor engaged by the Supplier to process Customer Personal Data on behalf of the Customer.

2. Scope and Customer Instructions

2.1 The subject matter, duration, nature and purpose of Processing, types of Personal Data and categories of Data Subjects are set out in Schedule 1.

2.2 The Supplier will process Customer Personal Data only on documented instructions from the Customer, including instructions in the Contract, this DPA, the applicable Order and the Customer's documented use/configuration of the processor feature.

2.3 If the Supplier is required by law to process Customer Personal Data other than on the Customer's instructions, it will inform the Customer before doing so unless the law prohibits that notification.

- 2.4 If the Supplier reasonably believes an instruction infringes Applicable Data Protection Law, it will inform the Customer and may suspend the affected Processing while the parties address the issue.
- 2.5 The Customer is responsible for the lawfulness of its instructions, the Personal Data it provides, its privacy notices and legal bases, and for ensuring instructions do not require the Supplier to violate applicable law.

3. Confidentiality and Personnel

- 3.1 The Supplier will ensure persons authorised to process Customer Personal Data are bound by confidentiality obligations or an appropriate statutory duty of confidentiality.
- 3.2 The Supplier will limit access to Customer Personal Data to personnel and Subprocessors who require access for the permitted Processing.

4. Security

- 4.1 Taking into account the state of the art, implementation costs, the nature, scope, context and purposes of Processing, and the risk to individuals, the Supplier will implement appropriate technical and organisational measures designed to ensure a level of security appropriate to risk.
- 4.2 Measures may include, as appropriate, access controls, authentication, encryption in transit and at rest where suitable, logging, vulnerability and patch management, backup and recovery, secure development practices, incident response, personnel access restrictions and periodic testing.
- 4.3 Schedule 2 describes the baseline security measures. The Supplier may update those measures where the overall level of protection is not materially reduced.

5. Subprocessors

- 5.1 The Customer gives the Supplier general authorisation to engage Subprocessors for the Processing.
- 5.2 The Supplier will maintain a current list of relevant Subprocessors and, where required by Applicable Data Protection Law, provide reasonable advance notice of a new Subprocessor so the Customer may object on reasonable data-protection grounds.
- 5.3 Where a valid objection cannot be resolved reasonably, the Supplier may offer an alternative that avoids the Subprocessor or, if no reasonable alternative is available, either party may terminate the affected processor feature without penalty as to the unperformed portion.
- 5.4 The Supplier will impose data-protection obligations on each Subprocessor that provide protection materially equivalent to the obligations applicable to the Supplier for the relevant Processing.
- 5.5 The Supplier remains responsible for its Subprocessors' performance of their processor obligations to the extent required by Applicable Data Protection Law.

6. Data Subject Rights

- 6.1 Taking into account the nature of the Processing, the Supplier will provide reasonable assistance by appropriate technical and organisational measures to help the Customer respond to requests from Data Subjects exercising their rights.
- 6.2 If the Supplier receives a request directly relating to Customer Personal Data, it will not respond substantively except on the Customer's documented instructions or where legally required, and will forward the request to the Customer where reasonably identifiable.

7. Personal Data Breaches

- 7.1 The Supplier will notify the Customer without undue delay after becoming aware of a Personal Data Breach affecting Customer Personal Data and will use reasonable endeavours, where reasonably practicable, to provide an initial notification within 24 hours of becoming aware. The 24-hour period is an operational notification target and does not delay the Supplier's obligation to notify without undue delay.
- 7.2 The notification will, as information becomes available, describe the nature of the breach, affected categories of data/individuals where known, likely consequences, mitigation steps, and a contact point for further information.
- 7.3 The Supplier will take reasonable steps to contain, investigate and remediate the breach. Notification under this clause is not an admission of fault or liability.
- 7.4 The Customer is responsible for determining whether notification to a regulator or Data Subjects is legally required, except where the Supplier has an independent legal obligation.

8. Assistance and Compliance

- 8.1 Taking into account the nature of Processing and information available to it, the Supplier will provide reasonable assistance to the Customer with security obligations, breach notifications, data-protection impact assessments and prior consultations with regulators where required.
- 8.2 Assistance that is materially beyond the ordinary Service may be charged at the Supplier's reasonable professional-services rates where permitted by law and agreed in advance.

9. Audits and Information

- 9.1 The Supplier will make available information reasonably necessary to demonstrate compliance with the processor obligations in Applicable Data Protection Law and this DPA.
- 9.2 Where reasonable, the parties will first use current security documentation, certifications, audit reports or questionnaires to satisfy audit requirements.
- 9.3 If additional audit is legally required or reasonably necessary following a material security incident or substantiated compliance concern, the Customer may conduct or appoint an independent auditor to conduct an audit on reasonable notice, during normal business hours and in a manner that protects other customers, security and confidential information.
- 9.4 The Customer bears its audit costs unless the audit identifies a material breach by the Supplier, in which case the Supplier will bear reasonable costs attributable to demonstrating remediation, subject to the liability terms of the Contract.

10. International Transfers

- 10.1 The Supplier will not make a Restricted Transfer of Customer Personal Data unless an applicable legal transfer mechanism is in place.
- 10.2 Where required for a UK Restricted Transfer, the parties will enter into or incorporate an appropriate UK International Data Transfer Agreement, UK Addendum to approved standard contractual clauses, adequacy mechanism or other legally recognised safeguard.
- 10.3 The Supplier may use Subprocessors in other countries only in accordance with Applicable Data Protection Law and the applicable transfer mechanism.

11. Return and Deletion

11.1 On termination of the relevant processor service, the Supplier will, at the Customer's choice and subject to the Service's technical capabilities, return or delete Customer Personal Data processed solely on behalf of the Customer, unless law requires continued retention.

11.2 The Supplier may retain secure backup copies for a limited period in accordance with normal backup cycles, provided retained data remains protected and is not restored except as required for disaster recovery, legal compliance or security.

11.3 This clause does not require deletion of information the Supplier lawfully processes in its separate capacity as controller, including contract, billing, security, fraud-prevention and legal evidence records.

12. Liability and Precedence

12.1 This DPA forms part of the Contract. The liability limitations and exclusions in the Contract apply to this DPA to the fullest extent permitted by law unless an Order expressly states otherwise.

12.2 If this DPA conflicts with the Contract on processor obligations, this DPA prevails for the affected Processing. If Schedule 1 conflicts with the main body of this DPA, the main body prevails unless Schedule 1 expressly states that a specific provision is varied.

12.3 Nothing in this DPA reduces any obligation or liability that cannot lawfully be excluded or restricted.

13. Term

13.1 This DPA starts when the Supplier begins processor Processing under the Contract and continues for so long as the Supplier processes Customer Personal Data on behalf of the Customer.

13.2 Clauses concerning confidentiality, security, deletion, audits and international transfers survive termination for so long as relevant Customer Personal Data is retained.

Schedule 1 — Processing Details

Subject matter	{{PROCESSOR_FEATURE_OR_SERVICE}}
Duration	For the duration of the relevant processor feature/order plus deletion/backup periods described in the Contract and this DPA.
Nature of Processing	{{NATURE_OF_PROCESSING}}
Purpose of Processing	{{PURPOSE_OF_PROCESSING}}
Categories of Data Subjects	{{DATA_SUBJECT_CATEGORIES}}
Types of Personal Data	{{PERSONAL_DATA_TYPES}}
Special-category/criminal data	Not intended unless expressly stated here: {{SPECIAL_CATEGORY_DATA_OR_NONE}}
Processing locations	{{PROCESSING_LOCATIONS}}
Customer instructions	The Contract, Order, this DPA and the Customer's documented configuration/use of the feature.

Schedule 2 — Baseline Technical and Organisational Measures

- Access controls based on least privilege and role requirements.
- Unique user/administrator credentials and suitable authentication controls.
- Encryption in transit using industry-standard transport encryption; encryption at rest where appropriate to the system and risk.
- Logging and monitoring of relevant authentication, administrative and security events.
- Patch, vulnerability and dependency-management processes proportionate to the Service.
- Secure software development and deployment practices.
- Backup, recovery and resilience arrangements proportionate to the Service.
- Incident response procedures and escalation paths.
- Confidentiality obligations and security awareness for personnel with relevant access.
- Supplier/subprocessor diligence appropriate to the nature and risk of the service.
- Data retention and deletion controls designed around the purpose of Processing.
- Periodic review and testing of security measures where appropriate.

Schedule 3 — Approved / Relevant Subprocessors

Populate this schedule with the actual providers used for the processor feature before using this DPA with a Customer. Do not list ordinary vendors merely because they exist in the wider business; list providers that process Customer Personal Data for the relevant processor service.

Subprocessor	Processing purpose	Location(s)	Transfer mechanism/status
{{SUBPROCESSOR}}	{{PURPOSE}}	{{LOCATION}}	{{MECHANISM_OR_NA}}
{{SUBPROCESSOR}}	{{PURPOSE}}	{{LOCATION}}	{{MECHANISM_OR_NA}}
{{SUBPROCESSOR}}	{{PURPOSE}}	{{LOCATION}}	{{MECHANISM_OR_NA}}
{{SUBPROCESSOR}}	{{PURPOSE}}	{{LOCATION}}	{{MECHANISM_OR_NA}}

Schedule 4 — Optional UK Restricted Transfer Mechanism

If a Restricted Transfer requires an additional UK transfer mechanism, attach or incorporate the applicable UK International Data Transfer Agreement, UK Addendum to approved standard contractual clauses, or other lawful transfer arrangement. Do not complete this schedule unless required for the actual Processing.

Implementation note: This DPA is a template for enterprise use and should be populated from the actual architecture, subprocessors and data flows. It should be legally reviewed before first use and rechecked if the product or applicable data-protection regime changes.