Rapid Risk Review

Data Processing Agreement

Last Updated: December 9, 2025

This Data Processing Agreement ("DPA") is entered into between the Customer ("Controller") and Rapid Risk Review ("Processor") and forms part of the Terms of Service or other agreement governing the use of RRR's vendor risk assessment platform.

1. Introduction and Scope

This DPA applies to the processing of Personal Data by the Processor on behalf of the Controller in connection with the provision of the Rapid Risk Review vendor risk assessment platform and related services (the "Services").

This DPA is designed to meet the requirements of Article 28 of the General Data Protection Regulation (GDPR) and other applicable data protection laws.

2. Definitions

- **"Personal Data"** means any information relating to an identified or identifiable natural person as defined under applicable Data Protection Laws.
- **"Processing"** means any operation performed on Personal Data, including collection, storage, use, disclosure, or deletion.
- **"Controller"** means the natural or legal person that determines the purposes and means of Processing Personal Data.
- **"Processor"** means the natural or legal person that Processes Personal Data on behalf of the Controller.
- **"Sub-processor"** means any third party engaged by the Processor to Process Personal Data on behalf of the Controller.
- **"Data Subject"** means the identified or identifiable natural person to whom Personal Data relates.

- **"Data Protection Laws"** means GDPR, CCPA, and other applicable privacy and data protection legislation.
- **"Security Incident"** means any unauthorized access, acquisition, use, or disclosure of Personal Data.

3. Subject Matter and Duration

3.1 Subject Matter

The Processor will Process Personal Data as necessary to provide the Services, which include:

- AI-powered vendor risk assessment and analysis
- Shadow IT and Shadow AI discovery through authorized integrations
- Team collaboration and workflow management
- Report generation and sharing
- Account management and customer support

3.2 Duration

This DPA shall remain in effect for the duration of the Controller's use of the Services and until all Personal Data has been deleted or returned in accordance with this DPA.

4. Nature and Purpose of Processing

The Processor will Process Personal Data solely for the purpose of providing the Services as described in the Terms of Service, including:

- User authentication and account management
- Storing and retrieving vendor risk assessments
- Processing Discovery integration data to identify third-party applications
- Facilitating team collaboration on risk assessments
- Generating and delivering reports
- Providing customer support

5. Types of Personal Data

Category	Data Elements
Account Information	Email address, full name, organization name, job title
Authentication Data	Hashed passwords, OAuth tokens (encrypted)
Usage Data	IP addresses, browser type, access timestamps, feature usage
Discovery Data	User email addresses associated with discovered applications
Payment Data	Billing email, subscription tier (card details handled by Stripe)

6. Categories of Data Subjects

- Customer employees with RRR platform accounts
- Customer employees identified through Discovery integrations
- Individuals whose contact information appears in vendor assessments

7. Processor Obligations

The Processor agrees to:

1. **Process Only on Instructions:** Process Personal Data only on documented instructions from the Controller, unless required by applicable law.
2. **Confidentiality:** Ensure that all personnel authorized to Process Personal Data are bound by confidentiality obligations.
3. **Security Measures:** Implement appropriate technical and organizational measures to protect Personal Data, as described in Section 9.
4. **Sub-processor Management:** Engage Sub-processors only with prior authorization and ensure they are bound by equivalent data protection obligations.
5. **Data Subject Rights:** Assist the Controller in responding to Data Subject requests for access, rectification, erasure, or portability.
6. **Breach Notification:** Notify the Controller of any Security Incident within 72 hours of becoming aware of it.

7. **Audit Cooperation:** Make available all information necessary to demonstrate compliance and allow for audits.
8. **Data Return/Deletion:** Upon termination, delete or return all Personal Data as directed by the Controller.

8. Controller Obligations

The Controller agrees to:

1. Provide lawful Processing instructions that comply with Data Protection Laws.
2. Ensure there is a valid legal basis for the Processing of Personal Data.
3. Fulfill transparency and notice obligations to Data Subjects.
4. Notify the Processor of any Data Subject requests received directly.
5. Conduct data protection impact assessments where required.

9. Security Measures

The Processor implements the following technical and organizational security measures:

9.1 Technical Measures

- **Encryption:** AES-256 encryption at rest, TLS 1.3+ encryption in transit
- **Access Controls:** Role-based access control (RBAC) with principle of least privilege
- **Authentication:** Multi-factor authentication (MFA) for administrative access
- **Network Security:** VPC isolation, firewalls, DDoS protection
- **Monitoring:** 24/7 security monitoring and intrusion detection
- **Backups:** Automated encrypted backups with point-in-time recovery

9.2 Organizational Measures

- **Personnel:** Background checks and security training for employees
- **Policies:** Information security policies and procedures
- **Assessments:** Annual penetration testing and security audits
- **Certifications:** SOC 2 Type II compliant infrastructure
- **Incident Response:** Documented incident response procedures

For complete details, see our Trust & Security Center.

10. Sub-processors

The Controller authorizes the use of the following Sub-processors:

10.1 Infrastructure Sub-processors

Sub-processor	Purpose	Location
Supabase	Database hosting, authentication	United States
AWS (Amazon Web Services)	Cloud infrastructure	United States
Lovable.dev	Development platform	European Union

10.2 Processing Sub-processors

Sub-processor	Purpose	Location
OpenAI	AI-powered risk analysis	United States
Google (Gemini)	AI-powered analysis	United States
Firecrawl	Web scraping for vendor analysis	United States
Trigger.dev	Background job processing	United States

10.3 Business Operations Sub-processors

Sub-processor	Purpose	Location
Stripe	Payment processing	United States
Resend	Transactional email delivery	United States
PDFShift	PDF report generation	European Union
Google reCAPTCHA	Bot protection	United States

10.4 Sub-processor Changes

The Processor will notify the Controller at least 30 days before adding or replacing Sub-processors. The Controller may object to such changes; if no resolution is reached, either party may terminate the affected Services.

11. Data Subject Rights

The Processor will assist the Controller in responding to requests from Data Subjects to exercise their rights under Data Protection Laws, including:

- Right of access
- Right to rectification
- Right to erasure ("right to be forgotten")
- Right to restriction of Processing
- Right to data portability
- Right to object

The Processor will notify the Controller promptly if it receives a request directly from a Data Subject.

12. Security Incident Notification

In the event of a Security Incident affecting Personal Data:

1. The Processor will notify the Controller within 72 hours of becoming aware of the incident.

2. The notification will include:
    - Description of the nature of the incident
    - Categories and approximate number of Data Subjects affected
    - Categories and approximate number of records affected
    - Likely consequences of the incident
    - Measures taken or proposed to address the incident
    - Contact point for further information
3. The Processor will cooperate with the Controller's investigation and regulatory notifications.

13. International Data Transfers

For transfers of Personal Data from the European Economic Area (EEA), United Kingdom, or Switzerland to countries not deemed adequate by the European Commission:

- The parties agree to the EU Standard Contractual Clauses (SCCs) for Controller-to-Processor transfers, which are incorporated by reference.
- The Processor will ensure Sub-processors are bound by equivalent transfer mechanisms.
- Additional safeguards include encryption and access controls as described in Section 9.

14. Audit Rights

The Controller has the right to audit the Processor's compliance with this DPA:

- **Self-Assessment:** The Processor will respond to reasonable security questionnaires annually.
- **Third-Party Audits:** The Processor will make available SOC 2 Type II reports upon request under NDA.
- **On-Site Audits:** Available for Enterprise customers with 30 days' notice, subject to confidentiality and reasonable scope limitations.

15. Term and Termination

15.1 Duration

This DPA is effective upon acceptance of the Terms of Service and remains in effect until the Services are terminated.

15.2 Data Return or Deletion

Upon termination of the Services:

- The Controller may export data via the platform's export features for 30 days.
- After 30 days, the Processor will delete all Personal Data within 90 days.
- Upon request, the Processor will certify deletion in writing.
- Personal Data may be retained as required by law, in which case it will be isolated and protected.

16. Liability

Liability under this DPA is subject to the limitations set forth in the Terms of Service, except that:

- Neither party excludes liability for breaches of Data Protection Laws that cannot be limited by contract.
- Each party remains liable for its own breaches and for the acts of its Sub-processors.

17. Standard Contractual Clauses

Where required for international transfers, the EU Standard Contractual Clauses (Commission Decision 2021/914) are incorporated by reference with:

- Module Two (Controller to Processor) applying
- The optional docking clause (Clause 7) included
- Option 2 of Clause 9(a) selected (general written authorization)
- The optional redress clause (Clause 11) not included
- Irish law governing the SCCs (Clause 17)
- Irish courts having jurisdiction (Clause 18)

Annex I (Details of Processing) and Annex II (Security Measures) are as described in Sections 3-6 and Section 9 of this DPA respectively.

18. Miscellaneous

- **Conflicts:** In case of conflict between this DPA and the Terms of Service, this DPA prevails for data protection matters.
- **Amendments:** This DPA may be updated to reflect changes in Data Protection Laws with 30 days' notice.
- **Severability:** If any provision is unenforceable, the remaining provisions remain in effect.
- **Entire Agreement:** This DPA, together with the Terms of Service and Privacy Policy, constitutes the entire agreement regarding data processing.

19. Contact Information

Rapid Risk Review

28 Geary Street, Ste 650 #1637
San Francisco, CA 94108
United States

- **Legal:** legal@rrr.dev
- **Privacy/DPO:** privacy@rrr.dev
- **Security:** security@rrr.dev

Need a customized DPA? Enterprise customers can request modifications to this standard DPA. Contact legal@rrr.dev to discuss your requirements.