DATA PROCESSING AGREEMENT

Between: ("**Data Controller**" or "**Customer**")
And: PlatoForms PTY Ltd. ("**Data Processor**" or "**PlatoForms**")

Effective Date:

1. DEFINITIONS

1.1 The following definitions apply to this Data Processing Agreement ("**DPA**"):

- **"Applicable Data Protection Laws"** means all applicable laws, regulations, and binding guidance relating to the processing of Personal Data, including without limitation the EU General Data Protection Regulation (GDPR), UK GDPR, California Consumer Privacy Act (CCPA), Australian Privacy Principles (APPs), and HIPAA where applicable.
- **"Data Subject"** means an identified or identifiable natural person to whom Personal Data relates.
- **"Personal Data"** means any information relating to an identified or identifiable natural person that is processed by PlatoForms on behalf of Customer under the Agreement.
- **"Processing"** means any operation performed on Personal Data, including collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure, dissemination, restriction, erasure, or destruction.
- **"Security Incident"** means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.
- **"Sub-processor"** means any third party engaged by PlatoForms to process Personal Data on behalf of Customer.

1.2 Terms not defined herein shall have the meaning ascribed to them in the main service agreement between the parties ("**Agreement**").

2. SCOPE AND APPLICABILITY

2.1 This DPA applies to all Processing of Personal Data by PlatoForms on behalf of Customer in connection with the Agreement.

2.2 This DPA supplements and forms part of the Agreement. In case of conflict between this DPA and the Agreement, this DPA shall prevail with respect to data protection matters.

2.3 The parties acknowledge that Customer is the Data Controller and PlatoForms is the Data Processor in respect of Personal Data processed under this DPA.

3. DATA PROCESSING DETAILS

3.1 Categories of Data Subjects:

- Form respondents and users
- Customer employees and representatives
- End-users of Customer's services
- Healthcare patients (where applicable under HIPAA compliance)

3.2 Categories of Personal Data:

- Contact information (names, email addresses, phone numbers)
- Identity data (IP addresses, device identifiers)
- Form submission data as configured by Customer
- Healthcare information (where Customer has enabled HIPAA compliance)
- Usage and analytics data

3.3 Processing Purposes:

- Provision of form creation and data collection services
- Data storage and management
- Analytics and reporting
- Customer support
- Legal compliance and security monitoring

3.4 Processing Duration:

Personal Data will be processed for the duration of the Agreement and retained according to Section 8 of this DPA.

4. DATA PROCESSOR OBLIGATIONS

4.1 Lawful Processing

PlatoForms shall process Personal Data only:

- On documented instructions from Customer (including this DPA)
- As necessary to comply with applicable legal obligations
- With Customer's prior written consent for any other purpose

4.2 Confidentiality

PlatoForms ensures that persons authorized to process Personal Data:

- Are bound by confidentiality obligations
- Receive appropriate training on data protection requirements
- Process Personal Data only as necessary for their roles

4.3 Security Measures

PlatoForms implements and maintains appropriate technical and organizational security measures, including:

Technical Safeguards:

- End-to-end encryption for data in transit and at rest
- Multi-factor authentication for system access
- Automated security monitoring and logging
- Regular security assessments and penetration testing
- AWS data centers with SOC 2 Type II compliance and multiple security certifications

Organizational Safeguards:

- Dedicated security officer responsible for HIPAA compliance
- Formal incident response procedures
- Employee security training and background checks
- Access controls based on need-to-know principles
- Regular policy reviews and updates

4.4 Sub-processing

- PlatoForms may engage Sub-processors in accordance with Section 6
- All Sub-processors must provide equivalent data protection guarantees
- Customer will be notified of Sub-processor changes with opt-out rights

5. DATA SUBJECT RIGHTS

5.1 PlatoForms shall assist Customer in fulfilling Data Subject rights requests, including:

- Right of access and data portability
- Right to rectification and erasure
- Right to restriction of processing
- Right to object to processing

5.2 PlatoForms will forward any Data Subject requests received directly to Customer within 2 business days.

5.3 PlatoForms will provide reasonable assistance to Customer in responding to requests within applicable legal timeframes.

6. SUB-PROCESSORS

6.1 Current Sub-processors:

Customer acknowledges and consents to PlatoForms' use of the following Sub-processors:

- Cloud infrastructure providers (AWS)
- CDN and security services providers (Cloudflare)
- Email delivery services (AWS)
- Payment processing providers (Stripe)
- Analytics and monitoring tools (Cloudflare)

6.2 Sub-processor Changes:

- PlatoForms will provide 30 days' written notice of new Sub-processors
- Customer may object to new Sub-processors with legitimate data protection concerns
- If Customer objects, parties will work together to find a solution or Customer may terminate the affected service

6.3 Sub-processor Requirements:

All Sub-processors must:

- Enter into written agreements with equivalent data protection obligations
- Implement appropriate technical and organizational security measures
- Comply with applicable data protection laws

7. INTERNATIONAL TRANSFERS

7.1 Personal Data may be transferred to and processed in countries outside the Customer's jurisdiction, including:

- United States (with appropriate safeguards)
- European Economic Area
- Australia

7.2 For transfers requiring additional safeguards under applicable law, PlatoForms will implement:

- Standard Contractual Clauses as approved by relevant authorities
- Adequacy decisions where available
- Other legally recognized transfer mechanisms

7.3 PlatoForms will maintain current transfer impact assessments and implement supplementary measures where required.

8. DATA RETENTION AND DELETION

8.1 Retention Period:

- Personal Data will be retained during the Agreement term
- After termination, data will be deleted within 90 days unless legally required to retain
- For HIPAA-compliant accounts, minimum 6-year retention applies where required

8.2 Data Return/Deletion:

Upon Customer request or Agreement termination, PlatoForms will:

- Provide data export in commonly used machine-readable format
- Securely delete all Personal Data from its systems
- Obtain deletion confirmation from Sub-processors
- Provide written certification of deletion upon request

8.3 Legal Hold:

PlatoForms may retain Personal Data longer if required by applicable law or legal proceedings, with prompt notification to Customer.

9. SECURITY INCIDENTS AND BREACH NOTIFICATION

9.1 Incident Response:

PlatoForms maintains a formal incident response plan and will:

- Detect and respond to Security Incidents without undue delay
- Contain and investigate incidents promptly
- Document all incident details and remediation steps

9.2 Breach Notification:

PlatoForms will notify Customer of Security Incidents:

- Without undue delay after becoming aware
- Within 24 hours for high-risk incidents
- Including all available information about the incident
- Providing regular updates as investigation progresses

9.3 Customer Cooperation:

PlatoForms will provide reasonable assistance to Customer for:

- Regulatory breach notifications
- Data Subject notifications
- Incident investigation and remediation

10. AUDITS AND COMPLIANCE

10.1 Documentation:
PlatoForms will maintain and provide upon request:

- Records of processing activities
- Security certifications and assessments
- Compliance documentation and audit reports

10.2 Audit Rights:
Customer may conduct audits of PlatoForms' data protection practices:

- Upon reasonable notice (minimum 30 days)
- No more than once annually unless required by incident or law
- At Customer's expense unless material non-compliance found
- Subject to confidentiality and security requirements

10.3 Third-Party Audits:
PlatoForms will obtain and share relevant third-party security certifications and rely on AWS infrastructure certifications (SOC 2, ISO 27001, FedRAMP) as evidence of compliance.

11. LIABILITY AND INDEMNIFICATION

11.1 Each party's liability under this DPA is subject to the limitation of liability provisions in the Agreement.

11.2 PlatoForms will indemnify Customer for direct damages resulting from PlatoForms' material breach of this DPA, subject to Agreement limitations.

11.3 Customer is responsible for:

- Ensuring lawful basis for processing
- Obtaining necessary consents and providing privacy notices
- Configuring services in compliance with applicable laws

12. TERM AND TERMINATION

12.1 This DPA becomes effective on the Effective Date and continues for the duration of the Agreement.

12.2 Either party may terminate this DPA for material uncured breach with 30 days' written notice.

12.3 Sections 8 (Data Retention), 9 (Security Incidents), and 11 (Liability) survive termination.

13. AMENDMENTS AND UPDATES

13.1 PlatoForms may update this DPA to reflect:

- Changes in applicable data protection laws
- New regulatory guidance
- Enhanced security measures

13.2 Material changes require 30 days' notice and Customer's continued use constitutes acceptance.

13.3 Customer may request DPA amendments through written notice, subject to mutual agreement.

14. GOVERNING LAW AND DISPUTES

14.1 This DPA is governed by the same law as the Agreement.

14.2 Disputes will be resolved according to the dispute resolution procedures in the Agreement.

14.3 Nothing in this DPA limits either party's rights under applicable data protection laws.

15. CONTACT INFORMATION

Data Protection Inquiries:
Email: privacy@platoforms.com
Address: 608 Harris Street Ultimo NSW 2007, Australia

Security Incidents:
Email: security@platoforms.com

ELECTRONIC SIGNATURE AGREEMENT

By electronically signing below, the parties agree to be bound by this Data Processing Agreement as of the Effective Date above.

PLATOFORMS PTY LTD.

By:	By:
Name:	Name:
Email:	Email:
Title:	Title:
Date:	Date:

APPENDIX A: TECHNICAL AND ORGANIZATIONAL MEASURES

A.1 ENCRYPTION

- **Data at Rest:** AES-256 encryption for all stored data
- **Data in Transit:** TLS 1.2+ for all data transmissions
- **Key Management:** Hardware security modules and regular key rotation

A.2 ACCESS CONTROLS

- **Multi-factor Authentication:** Required for all administrative access
- **Role-based Access:** Principle of least privilege applied
- **Access Logging:** All access attempts logged and monitored
- **Regular Reviews:** Quarterly access reviews and certifications

A.3 NETWORK SECURITY

- **Firewalls:** Next-generation firewalls with intrusion detection
- **VPN Access:** Required for remote infrastructure access
- **Network Segmentation:** Isolated environments for different data types
- **DDoS Protection:** Advanced threat protection and monitoring

A.4 INFRASTRUCTURE SECURITY

- **AWS Data Centers:** SOC 2 Type II, ISO 27001, and FedRAMP certified facilities
- **Physical Security:** Biometric access controls and 24/7 surveillance
- **Environmental Controls:** Climate and power redundancy systems
- **Geographic Distribution:** Multi-region backup and disaster recovery

A.5 APPLICATION SECURITY

- **Secure Development:** Security-by-design principles
- **Code Reviews:** Automated and manual security testing
- **Vulnerability Management:** Regular scanning and patch management
- **Penetration Testing:** Annual third-party security assessments

A.6 MONITORING AND INCIDENT RESPONSE

- **24/7 Monitoring:** Security operations center coverage
- **Automated Alerts:** Real-time threat detection and response
- **Incident Response Plan:** Documented procedures and escalation
- **Forensic Capabilities:** Log preservation and analysis tools

This Data Processing Agreement incorporates PlatoForms' existing HIPAA compliance framework and extends protection to meet global data protection requirements.