ExperiencePQ Data Processing Addendum (DPA)

Effective Date: 12 February 2026

This Data Processing Addendum ("**DPA**") forms part of the ExperiencePQ Terms of Use, SaaS Agreement, or any other agreement between you ("**Customer**") and ExperiencePQ Pty Ltd ABN 91694727109 ("**ExperiencePQ**", "**we**", "**us**", or "**our**") that governs your use of the ExperiencePQ platform and services (collectively, the "**Services**" and the "**Main Agreement**").

By using the Services, you agree to the terms of this DPA.

1 ROLES AND INSTRUCTIONS

1.1 You act as the **APP entity** (Controller) that determines the purposes and means of processing personal information.

1.2 ExperiencePQ acts as your **service provider** (Processor) and processes personal information only on your documented instructions and in accordance with this DPA and the Privacy Act 1988 (Cth).

1.3 This DPA contains your complete and final instructions for the processing of personal information. No additional instructions that would increase our obligations or costs will apply unless agreed in writing.

2 PROCESSING OF PERSONAL INFORMATION

2.1 We process personal information solely to provide, maintain, and improve the Services (e.g., lesson analysis, AI insights, team collaboration, performance tracking).

2.2 The nature, purpose, duration, types of personal information, and categories of data subjects are determined by how you use the Services. Typical examples include:

- Names, email addresses, and professional roles of users
- Debrief records, lessons learned, reflections, and action plans
- Activity logs and usage data

3 OUR OBLIGATIONS

We will:

3.1 Process personal information only on your documented instructions (including through the platform settings and this DPA).

3.2 Ensure that persons authorised to process personal information are bound by confidentiality obligations.

3.3 Implement and maintain appropriate technical and organisational measures to protect personal information (see **Annex A**).

3.4 Only engage sub-processors listed in **Annex B** (or with your prior written consent).

3.5 Assist you (at your reasonable cost) in responding to requests from individuals to exercise their rights under the Australian Privacy Principles (access under APP 12, correction under APP 13).

3.6 Notify you without undue delay (and no later than 72 hours where practicable) upon becoming aware of any actual or suspected eligible data breach.

3.7 Assist you with any required assessment and notification obligations under the Notifiable Data Breaches scheme.

3.8 At your direction, delete or return all personal information at the end of the Services (or within 30 days of termination), except where retention is required by law.

3.9 Make available all information reasonably necessary to demonstrate compliance with this DPA.

4 SUB-PROCESSORS

4.1 You authorise the sub-processors listed in **Annex B**.

4.2 We will give you at least 30 days' prior written notice of any intended addition or replacement of a sub-processor.

4.3 You may object to a new sub-processor within 14 days on reasonable data-protection grounds. If the objection is reasonable, we will work with you to find an alternative solution.

4.4 We remain fully liable to you for the acts and omissions of our sub-processors.

5 INTERNATIONAL TRANSFERS

5.1 Some sub-processors are located outside Australia (primarily the United States).

5.2 We take reasonable steps under **APP 8** to ensure overseas recipients do not breach the Australian Privacy Principles, including through contractual commitments in this DPA and sub-processor agreements.

5.3 Current sub-processors and locations are listed in **Annex B**.

6   DATA BREACHES

6.1 We will notify you without undue delay (and no later than 72 hours where practicable) of any actual or suspected data breach involving personal information.

6.2 The notification will include all information reasonably required for you to assess whether the breach is notifiable under the NDB scheme and to meet your obligations.

7   AUDITS

7.1 Upon your reasonable written request (no more than once per year, unless a breach has occurred), we will make available reports, certifications, or other evidence of compliance (e.g., SOC 2, penetration test summaries).

7.2 You may conduct an on-site or remote audit at your expense, subject to reasonable notice and confidentiality protections.

8   DATA DELETION

Upon termination of the Services, we will delete or return all personal information within 30 days, except where retention is required by law. You may request a data export in a standard format (JSON/CSV) at any time.

9   GOVERNING LAW

This DPA is governed by the laws of the Australian Capital Territory. The parties submit to the exclusive jurisdiction of the courts of the Australian Capital Territory.

By using the ExperiencePQ Services, you agree to this Data Processing Addendum.

ANNEX A: TECHNICAL AND ORGANIZATIONAL MEASURES

1. Access Control

- Multi-factor authentication (MFA)
- Role-based access control (RBAC)
- Row-level security (RLS)
- Session management and timeout
- IP allowlisting available on request

2. Data Security

- AES-256 encryption at rest

- TLS 1.2+ encryption in transit
- Secure key management
- Database-level encryption

3. Network Security

- Firewall protection
- Intrusion detection/prevention systems (IDS/IPS)
- DDoS mitigation
- Regular security patches

4. Physical Security

- Enterprise-grade data centers (Render, Google Cloud)
- Physical access controls
- Environmental monitoring
- Redundant power and cooling

5. Organizational Measures

- Security awareness training
- Background checks for personnel
- Confidentiality agreements
- Incident response procedures

6. Monitoring and Testing

- Continuous security monitoring
- Automated vulnerability scanning
- Third-party penetration testing (annual)
- Bug bounty program
- Audit logging

7. Backup and Recovery

- Automated daily backups
- Geographic redundancy
- Disaster recovery plan
- Regular restoration testing

8. Data Minimisation

- Collection limited to necessary data

- Automatic anonymization options for health data

- Retention policy enforcement

- Secure deletion procedures

ANNEX B: AUTHORIZED SUB-PROCESSORS

Sub-Processor	Service	Location	Purpose	Data Processing Addendum	Key Security Certifications
Base44 Ltd	Platform Infrastructure	USA	Application hosting and database	https://base44.com/dpa	SOC 2 Type II ISO 27001
Render	Server Hosting	USA	Compute and storage services	https://render.com/dpa	SOC 2 Type II ISO 27001:2022 HIPAA
Venice.ai	Artificial Intelligence	USA	AI Large Language Model.	https://venice.ai/legal/privacy-policy	No formal SOC 2 / ISO (privacy-by-design model)
Google Cloud Platform	Analytics Services	USA/EU	Data analytics and processing	https://cloud.google.com/terms/data-processing-addendum	SOC 2 (quarterly reports) ISO 27001, 27017, 27018
Mailgun (Sinch)	Email Delivery	USA	Transactional email services	https://sinch.com/es/legal/emea-terms/data-protection-agreement/	SOC 2 Type II ISO 27001 HIPAA
Daily.co	Video Conferencing	USA	Video call functionality	https://www.daily.co/legal/data-processing-addendum/	SOC 2 Type 2 Data centres: SOC 1/2 + ISO 27001 HIPAA
AssemblyAI	Speech Transcription	USA	Audio transcription services	https://www.assemblyai.com/legal/data-processing-addendum	SOC 2 Type 2 ISO 27001

Change Notification: The Processor will provide 30 days' written notice before adding or replacing Sub-processors. The Controller may object within 14 days.

ANNEX C: DATA SUBJECT REQUEST PROCEDURES

Access Requests:

- Controller submits request via Admin Panel or email

- Processor provides data within 30 days

- Format: JSON export via platform

Deletion Requests:

- Submitted through platform or by email

- Reviewed by Controller's admin

- Processor deletes within 30 days of approval

Rectification Requests:

- Controller updates data directly in platform

- Or submits request to Processor

- Changes implemented within 7 days

Portability Requests:

- Data exported in JSON format

- Available immediately through platform

For questions or DPA execution:
Leigh Anderson
leigh@experiencepq.io
ExperiencePQ