# Data Processing Agreement

**WisdomShift | GDPR Article 28 | Version 1.2 | Effective 1 December 2026**

This Data Processing Agreement ("DPA") forms part of the agreement under which the organisation identified in the acceptance record ("Controller") uses the WisdomShift platform (the "Services") provided by The ASPIRE Group International, LLC, 795 Waterbend Trail, Sarasota, Florida 34240, United States ("WisdomShift", "Processor"). It applies when the Controller's workspace administrator accepts it electronically, or when it is signed. The date and details of acceptance are recorded in the acceptance record, which forms part of this DPA.

## 1. Definitions

Terms such as "personal data", "processing", "controller", "processor", "data subject", "personal data breach" and "supervisory authority" have the meanings given in Regulation (EU) 2016/679 ("GDPR"). The same meanings apply under the UK GDPR and the Swiss FADP where relevant.

- **Applicable Data Protection Law**: GDPR, UK GDPR, the Data Protection Act 2018 (UK), the Swiss FADP, the Australian Privacy Act 1988 (Cth) and any other data protection law that applies to the processing under this DPA.
- **Workspace**: the account space in the Services administered by the Controller, including its coaches, learners and administrators.
- **Controller Personal Data**: personal data processed by WisdomShift on behalf of the Controller through the Workspace, as described in Annex I.
- **Sub-processor**: a third party engaged by WisdomShift to process Controller Personal Data.
- **Agreement**: the terms of service or subscription agreement between the parties.

## 2. Roles and scope

2.1 The Controller is the controller of Controller Personal Data and WisdomShift is its processor. Where the Controller itself acts as a processor for another party, WisdomShift is a sub-processor, and the Controller confirms it has authority to give the instructions in this DPA.

2.2 The subject matter, duration, nature and purpose of the processing, the types of personal data and the categories of data subjects are set out in Annex I.

2.3 The Controller is responsible for having a lawful basis for the processing, for giving data subjects the notices required by law, and for obtaining any consent that is required. This includes consent from every participant in a coaching session before it is recorded or transcribed.

2.4 The Controller will indemnify and hold harmless WisdomShift, its related entities, and their officers, employees, contractors and agents against all claims, losses, fines, penalties, damages and reasonable costs (including legal fees) arising from any session being recorded, transcribed or analysed through the Services without the notice or consent required by Applicable Data Protection Law or any call-recording law. This indemnity applies from the Controller's first use of the Services, including any free trial, and is not subject to any limitation of liability in the Agreement.

## 3. Processing on documented instructions

3.1 WisdomShift will process Controller Personal Data only on the Controller's documented instructions, including with regard to transfers to a third country, unless required to do otherwise by law to which WisdomShift is subject. In that case WisdomShift will tell the Controller of the legal requirement before processing, unless the law prohibits it.

3.2 This DPA, the Agreement, and the Controller's use and configuration of the Services are the Controller's complete documented instructions. Further instructions must be given in writing and may be declined where they are unreasonable or beyond the Services.

3.3 WisdomShift will tell the Controller promptly if, in its opinion, an instruction infringes Applicable Data

Protection Law.

3.4 WisdomShift will not process Controller Personal Data for its own purposes, will not sell or share it, and will not use it to train or fine-tune any general-purpose AI model. The only permitted derived use is anonymisation under clause 12.

## 4. Confidentiality

WisdomShift will ensure that every person authorised to process Controller Personal Data is bound by a duty of confidentiality, contractual or statutory, and receives appropriate data protection training. Access is limited to what each person needs to deliver the Services.

## 5. Security

5.1 WisdomShift will implement and maintain the technical and organisational measures in Annex II, taking into account the state of the art, the costs, the nature, scope, context and purposes of processing, and the risks to data subjects, as required by Article 32 GDPR.

5.2 WisdomShift may update the measures in Annex II from time to time, provided the overall level of protection is not reduced.

## 6. Sub-processors

6.1 The Controller gives general written authorisation for WisdomShift to engage the Sub-processors listed in Annex III.

6.2 WisdomShift will give the Controller at least 30 days' written notice (by email to the Workspace administrator and by update to the sub-processor page) before adding or replacing a Sub-processor. The Controller may object on reasonable data protection grounds within 14 days of notice. If the parties cannot resolve the objection in good faith, the Controller may terminate the affected Services without penalty and receive a pro rata refund of prepaid fees for the remaining term.

6.3 WisdomShift will bind each Sub-processor to data protection obligations no less protective than this DPA, and remains fully liable to the Controller for the Sub-processor's performance.

## 7. Data subject rights

7.1 Taking into account the nature of the processing, WisdomShift will assist the Controller, by appropriate technical and organisational measures, in responding to requests from data subjects to exercise their rights under Chapter III GDPR (access, rectification, erasure, restriction, portability, objection, and rights relating to automated decision-making).

7.2 If WisdomShift receives a request directly from a data subject about Controller Personal Data, it will not respond except to direct the person to the Controller, and will forward the request to the Controller promptly.

7.3 The Services include self-service export and deletion tools. Use of those tools is the preferred way to meet a request. Reasonable assistance beyond the tools will be provided at no charge unless it requires disproportionate effort.

## 8. Assistance with Articles 32 to 36

WisdomShift will assist the Controller in ensuring compliance with its obligations under Articles 32 to 36 GDPR (security, breach notification, data protection impact assessments and prior consultation), taking into account the nature of processing and the information available to WisdomShift. WisdomShift will provide the information the Controller reasonably needs to complete a data protection impact assessment for its use of the Services, including for any use of AI-assisted analysis of coaching sessions.

## 9. Personal data breach

9.1 WisdomShift will notify the Controller without undue delay, and in any event within 48 hours, after becoming aware of a personal data breach affecting Controller Personal Data.

9.2 The notice will, to the extent known, describe the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, the measures taken or proposed, and a contact point. Information may be provided in phases.

9.3 WisdomShift will take reasonable steps to contain and remediate the breach and will cooperate with the Controller's notification obligations to supervisory authorities and data subjects. A notification is not an admission of fault or liability.

## 10. Retention, deletion and return

10.1 WisdomShift handles Controller Personal Data in the classes described in Annex I, Part 5. Clause 10.1(a) applies throughout the term. If the Controller cancels the Services, clauses 10.1(b) to 10.1(e) also apply.

(a) **Raw audio and session transcripts.** Raw audio is streamed to the transcription Sub-processor while the session runs. WisdomShift does not store it: it is held only in server memory while the session and its post-session processing run, and is then discarded. Session transcripts are learner data. They are kept, encrypted, so the Services can show the learner's history and carry continuity between sessions. The Controller may set a shorter transcript retention period in its Workspace settings, or delete a transcript at any time. On cancellation, transcripts are deleted with the other learner data under clause 10.1(c).

(b) **Return window.** After the Controller confirms cancellation, a return window of 60 days applies. During the window the Controller may export its data using the export tools in the Services. The window cannot be shortened below 60 days.

(c) **Learner data, deleted at day 30.** Thirty days after the Controller confirms cancellation, WisdomShift will permanently delete all learner data. This includes learner records, sessions, learner-linked scores, session outputs, notes, consent records, learner settings, and knowledge base items taken from learner sessions. Learner names are also removed from retained logs and billing records. Learner data can therefore be exported only during the first 30 days of the return window. WisdomShift will issue a Learner Data Deletion Certificate, which the Workspace administrator can request at any time after the deletion.

(d) **Coach data, deleted at day 60.** At the end of the return window WisdomShift will permanently delete the coaches' own remaining data (knowledge base entries, personas, assessments, settings and files). WisdomShift will issue a final certificate covering both stages.

(e) **Backups.** Backups containing deleted data are overwritten within a further 35 days.

10.2 **Retained records.** WisdomShift keeps billing, tax, audit and compliance records, including deletion certificates, as required by law and for accountability. Learner names are removed from billing records. Audit and compliance records may hold a pseudonymous reference code, which remains personal data and is kept only as long as legally required. WisdomShift does not keep scores or other learner-linked data as permanent records.

10.3 After the retention periods above, WisdomShift will delete Controller Personal Data unless retention is required by law, in which case it will protect the data and process it only for that purpose.

## 11. Audit and information

11.1 WisdomShift will make available to the Controller all information necessary to demonstrate compliance with Article 28 GDPR, including current security documentation and, once available, summaries of independent audit reports (such as SOC 2).

11.2 The Controller may audit WisdomShift's compliance with this DPA once in any 12 month period, and additionally after a personal data breach or where required by a supervisory authority. Audits will be on at least 30 days' written notice, during business hours, subject to reasonable confidentiality obligations, and conducted so as not to disrupt WisdomShift's operations or compromise the data of other clients. WisdomShift may satisfy an audit request by providing independent audit reports or completed security questionnaires where these address the Controller's concerns. Each party bears its own costs.

## 12. Anonymised aggregate data

12.1 The Controller instructs WisdomShift to irreversibly anonymise Controller Personal Data so that it can no

longer be linked to any individual, directly or indirectly, using means reasonably likely to be used.

12.2 Anonymised data is generated only as aggregate outputs that meet a k-anonymity threshold of at least 10 and exclude names, contact details, free text and voice data. Anonymised data is not personal data and is not subject to this DPA. WisdomShift will not attempt to re-identify it and will contractually prohibit anyone it shares it with from doing so.

12.3 The act of anonymising is processing carried out as Processor under this DPA and the Controller authorises it.

12.4 Billing, tax, audit and compliance records are not anonymised data. They are kept under clause 10.2.

## 13. International transfers

13.1 WisdomShift stores Controller Personal Data in the United States (West), in the infrastructure of the Sub-processors listed in Annex III. The data residency setting in the Workspace records the Controller's stated preference and does not change where data is stored or processed. WisdomShift may also process Controller Personal Data in the other locations set out in Annex III, including AI and transcription processing in the United States, subject to clauses 13.2 and 13.3.

13.2 Where Controller Personal Data from the EEA, the UK or Switzerland is transferred to a country that has not received an adequacy decision, the parties agree that the Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914 apply and are incorporated into this DPA as follows: Module Two (controller to processor) between the Controller and WisdomShift; Clause 7 (docking) applies; in Clause 9 Option 2 (general authorisation) applies with the notice period in clause 6.2; in Clause 11 the optional language does not apply; in Clause 17 Option 1 applies and the governing law is that of Ireland; in Clause 18 the courts of Ireland. Annexes I, II and III to this DPA serve as Annexes I.A, I.B, II and III to the SCCs. For UK transfers the UK International Data Transfer Addendum (version B1.0) is incorporated. For Swiss transfers the SCCs apply with references to the GDPR read as references to the FADP and the Swiss Federal Data Protection and Information Commissioner as competent authority. The competent supervisory authority for the SCCs is the Irish Data Protection Commission.

13.3 WisdomShift will ensure each Sub-processor that receives data from outside the EEA is covered by an adequacy decision, the SCCs (Module Three) or another valid transfer mechanism, and will carry out transfer impact assessments where required.

13.4 If a transfer mechanism is invalidated, the parties will cooperate in good faith to put an alternative in place.

## 14. Government access requests

WisdomShift will notify the Controller of any legally binding request for disclosure of Controller Personal Data from a public authority, unless prohibited by law, will review each request for lawfulness and challenge it where there are reasonable grounds, and will disclose only the minimum permitted.

## 15. Liability

Each party's liability under this DPA is subject to the limitations and exclusions in the Agreement, except where applicable law does not permit them (including liability to data subjects under Article 82 GDPR and under the SCCs).

## 16. Term and termination

This DPA starts when accepted and continues for as long as WisdomShift processes Controller Personal Data. Clauses that by their nature should survive (including clauses 10, 11, 14 and 15) survive termination.

## 17. General

17.1 **Order of precedence.** In a conflict about the processing of personal data, the SCCs prevail, then this DPA, then the Agreement.

17.2 **Amendments.** WisdomShift may amend this DPA to reflect changes in law, supervisory authority guidance

or the Services. Material amendments will be notified at least 30 days in advance and a new version will be presented for acceptance. Each version is archived with a version number and content hash.

17.3 **Governing law.** Subject to the SCCs, this DPA is governed by the laws of the State of Florida, United States.

17.4 **Electronic acceptance.** The parties agree that acceptance by an authorised representative of the Controller through the Services, with the acceptance record captured, is a valid and binding signature. The person accepting confirms they have authority to bind the Controller.

17.5 **Contacts.** Data protection enquiries to WisdomShift: privacy@wisdomshift.app. WisdomShift has not appointed a data protection officer or an EU or UK representative.

---

## Annex I: Details of processing

**Part 1. Parties**

- Controller: as recorded in the acceptance record (organisation name, Workspace, accepting administrator, role, date). Role: controller.
- Processor: The ASPIRE Group International, LLC, trading as WisdomShift, 795 Waterbend Trail, Sarasota, Florida 34240, United States. Contact: privacy@wisdomshift.app. Role: processor.

**Part 2. Subject matter, nature and purpose**

WisdomShift provides an AI-assisted coaching platform. The processing includes:

- hosting Workspace accounts and coach and learner profiles;
- capturing and transcribing coaching sessions (live or uploaded), and telling the coach's speech apart from other speakers by the audio channel it arrives on (no voice profile is created);
- generating real-time prompts for the coach during sessions, drawn from the coach's own knowledge base;
- scoring sessions and tracking learner progress over time on the platform's effectiveness model;
- generating reports, summaries and coach development insights;
- sending service emails and notifications; and
- billing administration, security monitoring, support and diagnostics.

**Part 3. Duration**

For the term of the Agreement plus the retention periods in clause 10.

**Part 4. Categories of data subjects and personal data**

| Data subjects | Personal data |
|---|---|
| Coaches | Name, work email, role, organisation, credentials and accreditation details, profile content, knowledge base content, session performance data, usage and device data |
| Learners (the coaches' clients) | Name, work email, role, organisation, goals and coaching context, session content and derived records (themes, sentiment and engagement signals, scores, mindset stage), feedback |
| Workspace administrators | Name, work email, role, authentication and audit log data, jurisdiction and directory attributes (for example via SCIM) |
| Other session participants | Voice and speech content captured in a session, and anything they say |

Special categories: WisdomShift does not intentionally collect special category data. Two points need care. First, coaching conversations can include any topic, so special category data (for example health) may be disclosed by participants in session content. Second, session audio contains voices. WisdomShift does not create or store voice profiles, voiceprints or any other biometric template, does not use voice to identify a person, and does not store raw audio (clause 10.1(a)).

**Part 5. Data classes and retention**

| Class | Examples | Retention |
|---|---|---|

| | | |
|---|---|---|
| Raw audio | Session audio streamed for transcription | Not stored; held in server memory during processing only, then discarded |
| Session transcripts | Full session transcripts | Kept, encrypted, with the learner data. The Controller may set a shorter period or delete at any time. Deleted with learner data on cancellation (clause 10.1(c)) |
| Learner data | Learner records, sessions, learner-linked scores, session outputs, notes, consent records | Deleted 30 days after cancellation is confirmed (clause 10.1(c)) |
| Coach data | Knowledge base entries, personas, assessments, settings, files | Exportable and then deleted at day 60 (clause 10.1(d)) |
| Billing, tax, audit and compliance records | Cost and billing records, audit logs, deletion certificates | Kept as required by law, with learner names removed (clause 10.2) |
| Anonymised aggregate data | k-anonymous aggregate statistics (k = 10 or more) | Not personal data (clause 12) |

**Part 6. Frequency of transfer**

Continuous, for the term of the Agreement.

---

## Annex II: Technical and organisational measures

1. **Access control.** Role-based access with least privilege. Row-level security enforces Workspace isolation in the database. Staff access to Controller Personal Data is restricted, logged and reviewed. Multi-factor authentication is required for administrative and infrastructure accounts.
2. **Encryption.** TLS 1.2 or higher in transit. Encryption at rest for databases, object storage and backups. Session transcripts and session outputs are additionally encrypted by the application before they are stored. Secrets held in a managed secrets store and never in source code.
3. **Data minimisation and retention.** Raw audio is not stored. Transcripts are kept only as set out in Annex I, Part 5, and the Controller can set a shorter transcript retention period or delete transcripts. Only the data needed for the Services is kept. Automated deletion jobs enforce the retention periods in Annex I and produce deletion certificates.
4. **Jurisdiction handling.** The highest common standard is applied to all data (GDPR-grade controls regardless of user location). Jurisdiction is determined from Workspace directory data (for example SCIM), not inferred from email domains.
5. **AI processing controls.** Model providers are used under terms that prohibit training on Controller Personal Data and (where available) with zero or minimal data retention settings. Prompts to model providers are limited to what each task needs.
6. **Environment separation.** Production, development and test environments are separated. Production personal data is not used in development or testing.
7. **Logging and monitoring.** Security-relevant events are logged and monitored. Audit logs record administrative actions in the Workspace.
8. **Vulnerability management.** Dependencies are scanned. Security patches are applied on a risk-based schedule. Independent penetration testing is carried out before general release.
9. **Resilience and backup.** Regular encrypted backups, tested restoration, and a documented recovery process.
10. **Incident response.** A documented incident response plan with defined roles, and breach notification within the period in clause 9.
11. **Personnel.** Confidentiality undertakings, security and privacy training, and prompt removal of access when roles end.
12. **Vendor management.** Sub-processors are assessed before engagement and bound by written data protection terms.
13. **Compliance programme.** WisdomShift is building toward SOC 2 (including the Privacy criteria) and will

maintain records of processing, data protection impact assessments for its own platform design, and a documented compliance framework.

---

## Annex III: Authorised Sub-processors

*Last updated: 1 December 2026. Subscribers to the sub-processor notice list are told of changes under clause 6.2.*

| Sub-processor | Purpose | Data processed | Location |
|---|---|---|---|
| Supabase, Inc. | Database, authentication, storage | All Controller Personal Data at rest | United States (West) |
| Render Services, Inc. | Application hosting | Data in transit and in application memory | United States |
| Cloudflare, Inc. | Content delivery, DNS, web application firewall, edge workers | Request data, IP addresses | Global edge network |
| Anthropic, PBC | AI language model processing | Session content and prompts sent for analysis | United States |
| OpenAI, L.L.C. | AI language model processing | Session content and prompts sent for analysis | United States |
| Deepgram, Inc. | Speech-to-text transcription | Session audio | United States |
| Resend, Inc. | Transactional email delivery | Recipient name and email address, message content | United States |
| Stripe, Inc. | Subscription billing | Billing contact and payment details (Stripe also acts as an independent controller for its own regulatory purposes) | United States |