Data Processing Agreement

Azzm Tech · MIDDLE TRADER TELIFORM EA LTD, Dubai, UAE · Licence 870284
Version 1.0 · accepted electronically at registration

==========
==
DATA PROCESSING AGREEMENT (DPA)
Version 1.0
==========
==

BETWEEN

THE CENTRE: the therapy centre that creates an account on the Service ("Centre"). The Centre is identified in the acceptance record held by the Processor: centre name, administrator name and email, the version of this DPA accepted, and the date, time and IP address of acceptance.

AND

THE PROCESSOR: MIDDLE TRADER TELIFORM EA LTD, a sole establishment licensed in Dubai, United Arab Emirates, trade licence no. 870284, register no. 616398, whose registered address is Hor Al Anz, Dubai, United Arab Emirates, trading as "Azzm Tech" ("Processor" or "Azzm Tech")

(each a "Party", together the "Parties")

Effective date: the date the Centre accepts this DPA at registration.

BACKGROUND

A. The Processor provides a cloud software platform for therapy centres (the "Service"), including student records, programs, session data, progress tracking, documents and parent communication.

B. The Centre is a healthcare or therapy provider and is the controller of the personal data it enters into the Service, including special category / sensitive data relating to children.

C. The Parties wish to record the terms on which the Processor processes that data, as required by Article 28 of Regulation (EU) 2016/679 ("GDPR"), the UK GDPR, the UAE Personal Data Protection Law (Federal Decree-Law No. 45 of 2021, "PDPL") and other applicable laws.

D. This DPA forms part of, and is subject to, the agreement between the Parties for the Service (the "Principal Agreement"). In case of conflict on data protection matters, this DPA prevails.

---

1. DEFINITIONS

1.1 "Applicable Data Protection Law" means all laws applicable to the processing under this DPA, including the GDPR, the UK GDPR, the PDPL, and any implementing regulations, in each case as amended.

1.2 "Personal Data", "Processing", "Controller", "Processor", "Data Subject", "Personal Data Breach", "Special Category Data" and "Supervisory Authority" have the meanings given in the GDPR (and, for the PDPL, the corresponding meanings in that law).

1.3 "Centre Data" means all Personal Data that the Processor processes on behalf of the Centre under this DPA, as described in Annex A.

1.4 "Sub-processor" means any processor engaged by the Processor to process Centre Data.

1.5 "Restricted Transfer" means a transfer of Centre Data to a country or international organisation that does not benefit from an adequacy decision or other permitted transfer mechanism under Applicable Data Protection Law.

1.6 "Standard Contractual Clauses" or "SCCs" means the clauses annexed to Commission Implementing Decision (EU) 2021/914, Module Two (controller to processor).

1.7 "UK Addendum" means the International Data Transfer Addendum to the SCCs issued by the UK Information Commissioner under section 119A of the UK Data Protection Act 2018.

---

2. SCOPE AND ROLE

2.1 The Centre is the Controller of Centre Data and determines the purposes and means of processing. The Processor processes Centre Data only as a Processor and only on the Centre's documented instructions.

2.2 The subject matter, duration, nature and purpose of the processing, the categories of Data Subjects and Personal Data, and the applicable restrictions are set out in Annex A.

2.3 The Processor may process Centre Data for its own internal purposes only where it is itself a Controller under Applicable Data Protection Law (for example, statutory accounting records). It does not otherwise determine purposes or means.

2.4 The Processor is not a healthcare provider and does not exercise clinical judgement. The Centre remains responsible for the lawfulness of its processing, for its clinical decisions, and for its own notices to families.

---

3. PROCESSOR OBLIGATIONS

The Processor shall:

3.1 process Centre Data only on documented instructions from the Centre, including with regard to transfers to a third country, unless required to do so by law, in which case it shall inform the Centre of that legal requirement before processing, unless the law prohibits such information on important grounds of public interest;

3.2 ensure that persons authorised to process Centre Data are subject to appropriate confidentiality obligations (whether contractual or statutory);

3.3 implement and maintain the technical and organisational measures set out in Annex B, designed to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing, including protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access;

3.4 assist the Centre, by appropriate technical and organisational measures and insofar as possible, in fulfilling the Centre's obligation to respond to requests from Data Subjects exercising their rights, including access, rectification, erasure, restriction, portability and objection. The Processor shall not respond to such a request itself except to confirm that the request should be directed to the Centre, unless instructed otherwise;

3.5 assist the Centre in ensuring compliance with Articles 32 to 36 GDPR (and equivalent provisions of other Applicable Data Protection Law), taking into account the nature of the processing and the information available to the Processor, including data protection impact assessments and prior consultations with Supervisory Authorities;

3.6 notify the Centre without undue delay, and in any event within twenty-four (24) hours after becoming aware of a Personal Data Breach affecting Centre Data, providing the information described in Section 7;

3.7 at the Centre's choice, delete or return all Centre Data after the end of the provision of the Service, and delete existing copies, unless law requires storage. The parties agree that deletion is the default, as described in Section 9;

3.8 make available all information necessary to demonstrate compliance with this DPA and Article 28 GDPR, and allow for and contribute to audits, including inspections, by the Centre or a mandated auditor, as described in Section 10;

3.9 not engage any Sub-processor without the Centre's prior general written authorisation, and comply with Section 6 in respect of Sub-processors;

3.10 maintain records of its processing activities in accordance with Article 30 GDPR (and equivalent PDPL requirements) to the extent applicable;

3.11 where applicable, designate a data protection officer or privacy point of contact as required by Applicable Data Protection Law, and inform the Centre of any change;

3.12 not knowingly process Centre Data in a manner that infringes Applicable Data Protection Law, and inform the Centre immediately if, in its opinion, an instruction infringes such law.

---

4. CONTROLLER OBLIGATIONS

The Centre shall:

4.1 ensure that it has a lawful basis for the processing of Centre Data, including an Article 9 GDPR condition (or the PDPL equivalent) for sensitive health data, and that it has obtained and documented all necessary consents from parents or legal guardians;

4.2 ensure that its instructions to the Processor are lawful, and that the personal data it provides has been collected fairly and lawfully;

4.3 not instruct the Processor to process data for purposes outside the scope described in Annex A;

4.4 implement appropriate security measures for its own access credentials and devices, and manage user accounts, roles and deactivation;

4.5 provide families with its own privacy notice explaining the use of the platform, and handle Data Subject requests in the first instance;

4.6 be responsible for assessing whether a data protection impact assessment is required for its processing, and consult the Processor where necessary.

---

5. CONFIDENTIALITY AND PERSONNEL

5.1 The Processor shall take reasonable steps to ensure the reliability of any personnel who have access to Centre Data, and shall ensure they receive appropriate training on data protection and confidentiality.

5.2 Access shall be limited to personnel who need it to perform the Service or to provide support requested by the Centre, and shall be logged.

5.3 The Processor shall ensure that any personnel who leave its organisation, or change roles, no longer have access to Centre Data.

---

6. SUB-PROCESSORS

6.1 The Centre grants general written authorisation for the Processor to engage the Sub-processors listed in Annex C.

6.2 The Processor shall notify the Centre of any intended addition or replacement of Sub-processors at least thirty (30) days in advance, and shall give the Centre sufficient information to assess the change.

6.3 The Centre may object to the change on reasonable data protection grounds within the notice period. If the Parties cannot resolve the objection, the Centre may terminate the affected part of the Service without penalty and receive a pro-rata refund of prepaid fees for the unused period.

6.4 The Processor shall impose data protection obligations on each Sub-processor that are substantially the same as, and no less protective than, those in this DPA, and shall remain fully liable to the Centre for the acts and omissions of its Sub-processors.

6.5 The Processor shall provide a current list of Sub-processors on request and inform the Centre of the countries in which they process Centre Data.

---

7. PERSONAL DATA BREACHES

7.1 The Processor shall notify the Centre without undue delay, and in any event within twenty-four (24) hours after becoming aware of a Personal Data Breach affecting Centre Data.

7.2 The notification shall include, to the extent then known: 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 the contact point for further information. Where information is not available at the time of notification, it may be provided in phases without undue further delay.

7.3 The Processor shall take reasonable steps to mitigate the breach, and shall cooperate with the Centre in its notifications to Supervisory Authorities and Data Subjects.

7.4 The Processor shall not notify a Supervisory Authority or Data Subject on the Centre's behalf unless instructed in writing, except where required by law applicable to the Processor.

7.5 The Processor shall maintain an internal incident register recording the facts, effects and remedial action.

---

8. INTERNATIONAL TRANSFERS

8.1 The Processor may process Centre Data in the locations described in Annex C. The Centre acknowledges that the Service is delivered using infrastructure located in the United States, the European Union and other jurisdictions.

8.2 Where a Restricted Transfer is made, the Parties agree that:

(a) the SCCs (Module Two) are incorporated into this DPA by reference, with the Centre as "data exporter" and the Processor as "data importer", and with the following selections: Clause 7 (docking clause) - included; Clause 9 - Option 2, general written authorisation; Clause 11 - optional redress mechanism not included; Clause 17 - governing law of

Ireland; Clause 18 - courts of Dublin;

(b) where the UK GDPR applies, the UK Addendum is incorporated, with the Centre as "data exporter" and the Processor as "data importer", Table 1 completed with the Parties' details, Table 2 selecting the SCCs as amended by the Addendum, Table 3 listing Annex A and Annex C, and Table 4 selecting the Information Commissioner as regulator;

(c) where the PDPL applies, the transfer is made on a basis permitted by the PDPL and its implementing regulations, and the Processor shall cooperate in documenting that basis and obtain any approval required from the UAE Data Office;

(d) the Processor shall implement the supplementary measures described in Annex B and shall notify the Centre if it receives a legally binding request for disclosure from a public authority, unless prohibited by law.

8.3 The Processor shall challenge requests for access to Centre Data where it has reasonable grounds to believe the request is unlawful or overbroad, and shall seek to redirect the requesting authority to the Centre where lawful.

---

9. DELETION AND RETURN OF DATA

9.1 On termination or expiry of the Principal Agreement, or on the Centre's written request, the Processor shall delete Centre Data from live systems within thirty (30) days, and shall confirm deletion in writing on request.

9.2 The Processor may retain Centre Data (a) in encrypted backups that rotate out within thirty-five (35) days, and (b) where required by law, for the period required, subject to this DPA.

9.3 The Centre may export its Centre Data before termination using the export functionality of the Service, or by written request.

9.4 The Processor shall ensure that Sub-processors delete Centre Data on equivalent terms.

---

10. AUDIT AND COMPLIANCE

10.1 The Processor shall make available information reasonably necessary to demonstrate compliance with this DPA, including its security documentation, its sub-processor list and any relevant certifications.

10.2 The Centre may audit the Processor's compliance with this DPA not more than once in any twelve (12) month period, on at least thirty (30) days' written notice, during normal business hours, and subject to confidentiality. Where an audit would require access to other customers' data or to security-sensitive systems, the Processor may instead provide a report of an independent third-party audit or certification.

10.3 Audits shall be at the Centre's cost unless material non-compliance is found, in which case the Processor bears the reasonable cost.

10.4 Where a Supervisory Authority requires an inspection, the Processor shall cooperate as required by law.

---

11. LIABILITY AND INDEMNITY

11.1 CAP. Subject to Section 11.8, the Processor's total aggregate liability arising out of or in connection with this DPA, the Principal Agreement and the Service - whether in contract, tort (including negligence), breach of statutory duty, restitution or otherwise - shall not exceed the total fees actually paid by the Centre to the Processor in the twelve (12) months immediately preceding the event giving rise to the claim. Where no fees were paid, the cap is AED 1,000. Multiple claims shall not enlarge the cap.

11.2 EXCLUDED LOSSES. Subject to Section 11.8, neither Party is liable for indirect, incidental, special, punitive or consequential loss, or for loss of profit, revenue, goodwill, anticipated savings, business interruption, loss of use, loss of opportunity, or the cost of substitute services, even if that Party was advised of the possibility of such loss.

11.3 DATA LOSS. The Processor's responsibility for lost, corrupted or unavailable Centre Data is limited to using reasonable efforts to restore it from its backups. The Centre is responsible for exporting and retaining copies of records it must keep by law.

11.4 REGULATORY AMOUNTS. To the extent permitted by law, neither Party is liable for fines, penalties, compensation orders or assessments imposed on the other Party by a Supervisory Authority or other regulator.

11.5 DATA SUBJECT CLAIMS. Nothing in this DPA limits either Party's liability to a Data Subject under Article 82 GDPR (or equivalent provisions of other Applicable Data Protection Law), which is joint and several where both Parties are responsible for the same damage. As between the Parties, however:

(a) the Processor is responsible only for damage caused by its own breach of this DPA or of its direct obligations as a Processor;
(b) the Centre is responsible for damage caused by its own processing, its instructions, its failure to obtain a lawful basis or consent, or its breach of this DPA; and
(c) where one Party pays more than its share of a joint liability, it may recover the other Party's share, subject to the cap in Section 11.1.

11.6 CONTROLLER INDEMNITY. To the extent permitted by law, the Centre shall indemnify and hold harmless the Processor, its owner, employees and contractors against third-party claims, regulatory proceedings, losses and reasonable costs arising from:

(a) the Centre's processing of Centre Data, including clinical decisions, treatment and professional judgement;
(b) the Centre's failure to obtain or maintain any consent, notice or lawful

basis required for the processing, including guardian consent and any Article 9 (or PDPL equivalent) condition;
(c) instructions from the Centre that are unlawful or outside the scope of Annex A;
(d) content uploaded or entered by the Centre's users, including documents that infringe third-party rights; and
(e) the Centre's breach of this DPA, the Principal Agreement or Applicable Data Protection Law.

11.7 NO PERSONAL LIABILITY. Nothing in this DPA creates personal liability for the Processor's owner, directors, officers, employees or contractors in their individual capacity. This does not affect liability that cannot lawfully be excluded.

11.8 CARVE-OUTS. The limitations and exclusions in Sections 11.1, 11.2 and 11.4 do not apply to:

(a) fraud or fraudulent misrepresentation;
(b) wilful misconduct;
(c) death or personal injury caused by negligence;
(d) breach of confidentiality obligations in respect of Centre Data; or
(e) any liability that applicable law does not permit to be limited.

Where a carve-out applies, the Processor's liability for that head of loss shall be subject to a separate aggregate cap of two (2) times the amount in Section 11.1.

11.9 CLAIM PERIOD. To the extent permitted by law, a claim under this DPA must be notified within twelve (12) months of the date the claiming Party became aware, or ought reasonably to have become aware, of the circumstances giving rise to it. This does not shorten any period that cannot lawfully be shortened.

11.10 SEVERABILITY OF LIMITATIONS. Each limitation in this Section 11 operates separately. If any is held unenforceable, the remaining limitations apply, and the unenforceable limitation shall be replaced by the narrowest enforceable provision achieving a similar purpose.

11.11 INSURANCE. The Processor maintains the insurance it considers appropriate for its business and will describe its current cover on reasonable request.

---

12. TERM AND TERMINATION

12.1 This DPA takes effect on the effective date and continues until the Processor ceases to process Centre Data.

12.2 Sections 7, 9, 11, 13 and 14 survive termination.

12.3 A material breach of this DPA that is not remedied within thirty (30) days of written notice entitles the non-breaching Party to terminate the Principal Agreement and this DPA.

---

13. GENERAL

13.1 Governing law: this DPA is governed by the law of THE UAE, without prejudice to the SCCs and the UK Addendum, which are governed by their own terms.

13.2 Dispute resolution: the courts of Dubai, United Arab Emirates have exclusive jurisdiction, save that either Party may seek interim relief in any competent court.

13.3 Order of precedence: (1) the SCCs and UK Addendum; (2) this DPA; (3) the Principal Agreement; (4) the Processor's standard terms.

13.4 Entire agreement: this DPA and its Annexes constitute the entire agreement between the Parties on the processing of Centre Data.

13.5 Severability: if a provision is held invalid, the remainder continues in effect and the Parties shall replace the invalid provision with one achieving the same purpose.

13.6 Amendments: no amendment is effective unless in writing and signed by both Parties.

13.7 No third-party beneficiaries: no person other than the Parties has any right to enforce this DPA, except a Data Subject exercising rights under Applicable Data Protection Law.

13.8 Entire liability: this DPA, the Principal Agreement and the SCCs / UK Addendum set out the Parties' entire liability for the processing, and replace any prior representations on that subject.

SIGNATURES

For the Controller:

Name: _____
Title: _____
Signature: _____
Date: _____

For the Processor:

Name: _____
Title: _____
Signature: _____
Date: _____

==========

ANNEX A - DETAILS OF PROCESSING

==========

==

A.1 Subject matter

Provision of a cloud platform for therapy centre management, including student records, program and target tracking, session data collection, progress reporting, document storage and parent communication.

A.2 Duration

The term of the Principal Agreement, plus the retention periods described in Section 9.

A.3 Nature of processing

Collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, disclosure by transmission within the Service, alignment, combination, restriction, erasure and destruction. Processing is automated and includes database storage, file storage and document text extraction.

A.4 Purposes

(a) Providing the Service to the Centre and its authorised users.
(b) Maintaining, securing, backing up and supporting the Service.
(c) Producing reports and summaries requested by the Centre.
(d) Complying with the Processor's own legal obligations.

A.5 Categories of Data Subjects

(a) Children and young persons receiving therapy at the Centre.
(b) Parents and legal guardians.
(c) Centre staff, therapists, supervisors and administrators.

A.6 Categories of Personal Data

(a) Identification: name, date of birth, student ID, photograph, guardian contact details.
(b) Special category / sensitive data: diagnoses, therapy programs and targets, trial and behaviour data, speech and language samples, sensory and motor assessments, academic and reading-fluency scores, assessment results (VB-MAPP, ABLLS-R), session notes, reports, supervisor sign-offs.
(c) Documents and messages, including extracted document text with names replaced by student ID.
(d) Account data for staff and parents: name, email, role, centre, authentication data.
(e) Technical data: IP address, browser information, timestamps, error logs.

A.7 Special category data

Yes. Health and therapy data relating to children. The Centre is responsible for identifying and documenting its Article 9 condition (or PDPL equivalent) and for guardian consent.

A.8 Frequency of transfer

Continuous, for the duration of the Service.

A.9 Retention

As determined by the Centre while the account is active; deletion within 30 days of termination or request; backups within 35 days.

A.10 Sub-processor processing

As set out in Annex C.

A.11 Sensitive-data safeguards

Role-based access, centre isolation, encryption in transit and at rest, de-identification of extracted document text, audit logging, and daily encrypted backups.

==========

ANNEX B - TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

==========

B.1 Access control

- Unique user accounts; no shared credentials.
- Role-based permissions: therapists (assigned students), supervisors (caseload), centre administrators (their centre), parents (their children), platform administrators (support, logged).
- Centre-level tenant isolation.
- Deactivation of accounts on staff departure, at the Centre's instruction.

B.2 Authentication and credentials

- Passwords stored as salted one-way hashes.
- Time-limited access and refresh tokens.
- Password reset via single-use, time-limited tokens.
- Two-factor authentication (TOTP) available to centre administrator accounts, with single-use recovery codes and per-account enrolment records.

B.3 Encryption

- TLS/HTTPS for all traffic in transit.
- Encryption at rest provided by the hosting, database and storage providers.
- Encrypted backups: daily database dump, retained for up to 35 days by an enforced bucket lifecycle rule, with a weekly automated restore drill whose dated evidence record is retained alongside the backups.

B.4 Availability and resilience

- Daily automated database backups to encrypted object storage.
- Periodic restore testing.
- Backups retained for up to 35 days.

B.5 Data minimisation and de-identification

- Document text extraction replaces child and guardian names with the student ID before storage.
- Parent portal displays only the Centre's configured fields, and only the parent's own children.

B.6 Logging and monitoring

- Error and security logging with retention up to 90 days.
- Support access limited and logged.

B.7 Personnel

- Confidentiality obligations for all personnel.
- Access granted on a need-to-know basis.

B.8 Sub-processor management
- Written data protection terms with each Sub-processor.
- Annual review of Sub-processor security posture.

B.9 Incident response
- Documented incident handling with notification to the Centre within 24 hours of confirmation.
- Post-incident review and remediation.

B.10 Secure development
- Source code hosted with access controls.
- Dependency and secret management practices.

==========
ANNEX C - AUTHORISED SUB-PROCESSORS
==========

Sub-processor	Processing	Location
Vercel	Web application hosting and delivery	US / global edge
Render	Application server, background jobs	US
Neon	Managed Postgres database	US
Cloudflare	DNS; R2 object storage; backups	Global / US
Resend	Transactional email	US
Stripe	Subscription billing, card processing	US / Ireland
GitHub	Source code; scheduled backup execution	US

Note: OpenAI-compatible OCR is not enabled by default. If an external recognition provider is enabled, this Annex will be updated and notice given under Section 6.2 before it processes live Centre Data.

==========
END OF DATA PROCESSING AGREEMENT
==========