Data Processing Agreement

This Data Processing Agreement ("DPA") forms part of the Terms of Service between you, the therapist ("the Controller"), and **A Possible Space Ltd.** ("the Processor", "we", "us"), and governs our processing of personal data about your clients when you use **Parts**. Where this DPA and the Terms conflict on data protection, this DPA prevails.

- **Processor:** A Possible Space Ltd., company number 11617016, VAT number GB364357384, registered in England & Wales, registered office: The Old Bakery, 90 Camden Road, Tunbridge Wells, England, TN1 2QP.
- **Contact:** us@possible.space.
- **Effective date:** 2026-06-10. **Version:** 2026-06-05.

1. Roles

You are the **controller** of your clients' personal data. We are the **processor**, acting only on your documented instructions. "Data protection law" means the UK GDPR, the Data Protection Act 2018, and (where it applies) the EU GDPR. Terms such as "personal data", "special category data", "processing", and "data subject" have the meanings given in that law.

2. Our obligations

In plain terms, this section is our promise about how we handle your clients' data: we only do what you tell us, we keep it confidential and secure, we help you answer your clients' requests, and we tell you quickly if anything goes wrong. Precisely, we will:

1. process your clients' personal data **only on your documented instructions** (using Parts as intended is your instruction), including as to international transfers, unless the law requires otherwise, in which case we'll tell you first unless prohibited;
2. ensure that people authorised to process the data are under a duty of **confidentiality**;
3. implement appropriate **technical and organisational security measures** (Annex 3), proportionate to the sensitivity of the data;
4. **assist you** in responding to your clients' requests to exercise their rights (access, rectification, erasure, portability, restriction, objection), including by providing an export in time for you to meet your own statutory deadline;
5. assist you with your obligations around **security, breach notification, data protection impact assessments** (a formal risk check you may have to do), and prior consultation with the ICO under Article 36;
6. **notify you without undue delay** after becoming aware of a personal-data breach affecting your data, and promptly enough to allow you to meet your own 72-hour notification deadline to the ICO;
7. at your choice, **delete or return** your clients' personal data at the end of the service (clause 7); and
8. make available the information necessary to **demonstrate compliance** with this DPA, and allow for audits (clause 6).

We provide the assistance in points 4 and 5 at no additional charge.

3. Your warranties

As the controller, you warrant that, for the client data you record in Parts, you: have a valid lawful basis under Article 6 and a condition under Article 9 for special-category (health) data; have obtained any necessary **parental or guardian consent** where a client is a child; and have given your clients the privacy information the law requires (Articles 13-14). We rely on these warranties in processing the data for you.

4. The processing (Article 28 details)

- **Subject-matter:** provision of the Parts mapping service.
- **Duration:** for as long as you use Parts, plus the deletion period in clause 7.
- **Nature and purpose:** storing, organising, versioning, and displaying the Maps you create, so you can review your clinical work between sessions.
- **Types of personal data:** the content of Maps — Part types, labels, descriptions, body locations, free-text notes, positions, and the Relationships between Parts, together with their change history. This is **special-category data concerning health**, and may include data about **children**.
- **Categories of data subjects:** your **clients**.

5. Sub-processors

You give us **general authorisation** to engage sub-processors. Our current sub-processors are listed in Annex 2. We impose data-protection obligations on each sub-processor equivalent to those in this DPA, and we remain responsible for their performance.

We will give you at least **14 days' notice** before a new or replacing sub-processor begins processing your data, and it will **not begin** until that notice period has passed. You may object on reasonable data-protection grounds; if we can't resolve your objection, you may terminate by ceasing to use Parts and requesting deletion, and we will **refund any prepaid fees for the unused remainder** of your period.

6. Audits

We will make available the information needed to demonstrate compliance with this DPA. You may also audit our compliance, on at least **30 days' written notice**, no more than **once a year** (unless a regulator requires it or following a breach), during business hours, subject to confidentiality, with each party bearing its own costs.

7. Return and deletion

On termination, or at your request, we will **delete** (or, at your choice, return) your clients' personal data within **30 days**, except where the law requires us to keep it. Data in encrypted backups is purged as those backups age out, within **30 days**.

8. International transfers

Primary processing and backups are in the **EU**. Where a sub-processor is outside the UK/EEA (Annex 2), transfers are protected by appropriate safeguards — the UK International Data Transfer Agreement / EU Standard Contractual Clauses, and, for Stripe, the EU-US and UK Data Privacy

Framework. We will not make onward transfers without an appropriate safeguard. You can ask us for a copy of the relevant safeguard at us@possible.space.

9. Liability

The limitations and exclusions of liability in the Terms of Service apply to this DPA. Nothing in this DPA or the Terms limits either party's liability to a **data subject** under data-protection law, or any liability that cannot be limited by law.

10. Term and governing law

This DPA lasts as long as we process your clients' data. It is governed by the law of **England & Wales**.

Annex 1 — Details of processing

As set out in clause 4 above.

Annex 2 — Sub-processors

These are the providers that process your **clients' data** on our behalf:

Sub-processor	Purpose	Location
Hetzner Online GmbH	Hosting and database	Falkenstein, Germany (EU)
Scaleway	Encrypted off-site backups	Paris, France (EU)

The other providers we use — **Stripe** (payment processing), **Fastmail** (email), and **Plausible** (website analytics) — process **our own** data about you (billing, contact, and website-visit data, for which we are the controller), not your clients' data, so they are not sub-processors under this DPA. They are listed in the Privacy Policy.

Annex 3 — Security measures

- **Encryption** in transit (HTTPS) and at rest; encrypted off-site backups that are encrypted before they leave our systems, so the backup provider cannot read them, with the backup encryption key kept separate from the backup data.
- **Access controls** limiting access to authorised, named personnel on a least-privilege basis, and scoping each therapist's Maps to that therapist.
- **Confidentiality** undertakings binding staff and contractors.
- **Logging and monitoring** of changes to clinical records (an audit log).
- A dedicated, **restricted code path for erasure** (the right to be forgotten).
- **Data minimisation in operations:** operational logs and operator alerts exclude clinical content — only structural identifiers and error metadata are recorded, never a client's notes or other Map content.

Changes to this agreement

- **2026-06-05** — Initial version.