

DATA PROCESSING ADDENDUM (DPA)

This Data Processing Addendum ("DPA") forms part of the Master Services Agreement or other written or electronic agreement (the "Agreement") between Polso Limited ("Polso" or "Processor") and the Customer ("Customer" or "Controller") for the provision of the Services.

1. Definitions and Interpretation

"Data Protection Laws" means all applicable worldwide privacy and data protection laws and regulations, including the UK GDPR, the Data Protection Act 2018, and the EU GDPR.

"Customer Data" means any Personal Data processed by Polso on behalf of the Customer in the course of providing the Services (as detailed in Annex 1).

Terms such as **"Controller"**, **"Processor"**, **"Data Subject"**, **"Personal Data"**, **"Personal Data Breach"**, and **"Processing"** shall have the meanings given to them in the Data Protection Laws.

2. Roles and Scope

- 2.1. In respect of Customer Data, the parties acknowledge that Customer is the Controller (or a Processor acting on behalf of a third-party Controller) and Polso is the Processor.
- 2.2. This DPA applies exclusively to the processing of Customer Data. It does not apply to business contact information or administrative data where Polso acts as an independent Controller (as governed by the Polso Privacy Policy).

3. Processing Instructions

- 3.1. Polso shall process Customer Data only on the documented instructions of the Customer, unless required to do otherwise by applicable law.
- 3.2. The Agreement (including the applicable Order Form) and this DPA constitute the Customer's complete and final instructions to Polso. Any additional or alternate instructions must be agreed upon in writing. Polso reserves the right to charge additional fees to comply with custom processing instructions.

4. Customer Obligations

- 4.1. The Customer warrants that it has all necessary rights, consents, and lawful bases to provide the Customer Data to Polso for the Processing contemplated by the Agreement.
- 4.2. The Customer is solely responsible for its own compliance with Data Protection Laws and for the accuracy, quality, and legality of the Customer Data.

5. Sub-processing

- 5.1. **General Authorization.** Customer provides general written authorization for Polso to engage third-party sub-processors to process Customer Data.
- 5.2. **Changes.** Polso shall notify the Customer (e.g., via email or an in-app notification/status page) at least 30 days before appointing a new sub-processor.
- 5.3. **Objections.** If the Customer objects to a new sub-processor on reasonable data protection grounds within 14 days of notice, the parties will discuss a resolution in good faith. If the parties cannot resolve the objection, Polso may, at its discretion, allow the Customer to terminate the affected Services without penalty.

6. Security & Confidentiality

- 6.1. Polso shall implement and maintain appropriate technical and organisational measures designed to protect Customer Data against accidental or unlawful destruction, loss, alteration, or unauthorised disclosure or access.
- 6.2. Polso shall ensure that all personnel authorised to process Customer Data are bound by appropriate obligations of confidentiality.

7. Personal Data Breaches

- 7.1. If Polso becomes aware of a confirmed Personal Data Breach affecting Customer Data, Polso shall notify the Customer without undue delay.
- 7.2. Polso will provide reasonable information and cooperation to the Customer to assist the Customer in fulfilling its data breach reporting obligations under Data Protection Laws. Polso's notification of a breach shall not be construed as an acknowledgement of fault or liability.

8. Data Subject Requests

- 8.1. If Polso receives a request from a Data Subject regarding their Customer Data (e.g., access, deletion, or rectification), Polso will not respond directly to the request (unless required by law) and will instead promptly forward the request to the Customer.
- 8.2. Taking into account the nature of the processing, Polso will provide the Customer with reasonable assistance (e.g., via platform functionality) to enable the Customer to respond to such requests.

9. Audits and Inspections

- 9.1. To verify compliance with this DPA, Customer shall first request and review Polso's most recent security documentation or compliance reports.
- 9.2. Only if such documentation is reasonably insufficient to demonstrate compliance, the Customer may request to conduct a remote audit or questionnaire no more than once per calendar year. Any such audit must be conducted during regular

business hours, subject to confidentiality obligations, and strictly at the Customer's own expense.

10. International Data Transfers

- 10.1. Polso shall not transfer Customer Data outside the UK or European Economic Area (EEA) unless it has taken measures necessary to ensure the transfer is compliant with Data Protection Laws.
- 10.2. If Customer Data is transferred to a country not recognized as providing an adequate level of protection, the parties agree that the applicable standard contractual clauses (e.g., the UK International Data Transfer Addendum or EU SCCs) shall be deemed incorporated into this DPA by reference, with Polso acting as the data importer.

11. Deletion or Return of Data

Upon termination or expiry of the Agreement, Polso shall, at the Customer's choice, delete or return all Customer Data to the Customer within thirty (30) days, unless applicable law requires continued storage of the Customer Data.

12. Limitation of Liability

Any claims, damages, or liabilities arising out of or in connection with this DPA (including any standard contractual clauses incorporated herein) shall be subject to the exclusions and limitations of liability set out in the main Agreement.

ANNEX 1: DETAILS OF PROCESSING

Subject Matter and Duration of Processing	Polso processes Customer Data for the purpose of providing the SaaS services to the Customer as described in the Agreement, for the duration of the applicable Subscription Period.
Nature and Purpose of Processing	Computing, storing, transmitting, and analyzing data to provide customer retention, product telemetry, and analytics services as configured by the Customer via the Software.
Categories of Data Subjects	The Customer's employees, personnel, and authorized users accessing the Software; the Customer's end-users interacting with the Customer's own products (generating telemetry); and the Customer's business contacts, clients, and account stakeholders (such as sponsors or champions) whose profile or engagement data is submitted to the Software.
Types of Personal Data Processed	User identifiers (e.g., user IDs, names, email addresses), device information, IP addresses, software interaction data (telemetry logs), and any other Personal Data that the Customer chooses to upload or connect to the Polso platform via integrations or APIs.