# PABAU DATA PROCESSING AGREEMENT

This Data Processing Agreement (the Agreement) forms part of the agreement between:

Hambrand Technology Limited, a company incorporated in England and Wales, trading as Pabau (the Processor); and

The customer identified in the applicable order form, subscription, or acceptance of the Pabau Terms of Use (the Controller).

Together, the Parties.

## 1. Definitions

**1.1** Capitalised terms not otherwise defined in this Agreement shall have the meanings given to them in the UK GDPR, the GDPR, and the Pabau Terms of Use.

**1.2** UK GDPR means the United Kingdom General Data Protection Regulation as incorporated into UK law by the Data Protection Act 2018.

## 2. Scope and Purpose of Processing

**2.1** The Processor shall process Personal Data solely for the purpose of providing the Pabau software platform and related services to the Controller.

**2.2** The subject matter, duration, nature, and purpose of the processing, together with the types of Personal Data and categories of Data Subjects, are described in Annex A.

## 3. Controller Instructions

**3.1** The Processor shall process Personal Data only on documented instructions from the Controller, including with regard to transfers of Personal Data to a third country or international organisation, unless required to do so by applicable law.

**3.2** Where the Processor is required by law to process Personal Data otherwise than on the Controller's instructions, the Processor shall inform the Controller of that legal requirement unless prohibited by law.

## 4. Confidentiality

**4.1** The Processor shall ensure that persons authorised to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

## 5. Security of Processing

**5.1** The Processor shall implement appropriate technical and organisational measures 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.

**5.2** Such measures are described in Annex B.

## 6. Sub Processors

**6.1** The Controller authorises the Processor to engage Sub Processors to process Personal Data, including those listed in Annex C.

**6.2** The Processor shall impose data protection obligations on Sub Processors that are no less protective than those set out in this Agreement.

**6.3** The Processor will maintain an up-to-date list of Sub-processors (available via our website/terms). The Data Controller will be informed of any new Sub-processor by the posting of an updated list. If the Controller objects to a new Sub-processor on reasonable grounds, it may terminate the service. No specific prior notice period is guaranteed.

## 7. International Transfers

**7.1** Data Location: All personal data for UK customers will be stored and processed on servers located in the UK. Data will only be transferred outside the UK if required for specific sub-processor services, and any such transfers shall be subject to UK GDPR-compliant Standard Contractual Clauses and equivalent safeguards.

## 8. Assistance with Data Subject Rights

**8.1** Taking into account the nature of the processing, the Processor shall assist the Controller by appropriate technical and organisational measures to enable the Controller to fulfil its obligations to respond to requests for exercising Data Subject rights.

**8.2** Audit logs of user activity are retained for 1 month and can be accessed/exported by the Controller upon request for compliance and investigation purposes.

**8.3** The Controller may export audit trail logs or request an export in a common format (CSV/Excel) for their own compliance needs.

**8.4** Upon Controller's request (e.g., to fulfil a data subject's erasure request), the Processor will facilitate the deletion of the specified individual's record from the live system, provided that such deletion is consistent with the Controller's obligations (e.g., no overriding legal requirement to retain the data).

## 9. Personal Data Breaches

**9.1** The Processor shall notify the Controller without undue delay and in any event within 24 hours after becoming aware of a Personal Data Breach.

**9.2** The Processor will promptly provide the Controller with all information it has about the breach to enable the Controller to comply with any 72-hour breach notification obligations to the ICO, including the nature of the breach, affected data categories, approximate volumes, consequences, and

mitigation measures taken.

## 10. Deletion or Return of Personal Data

**10.1** Upon termination: any AI-generated transcripts that form part of the medical record will be included in the data export provided to the Controller, and any associated audio files or intermediate AI data will be permanently deleted in line with Clause 10.

**10.2** When a record is deleted upon request, it will be expunged from production systems. Any remnants in encrypted backups will be overwritten in the normal backup rotation cycle.

## 11. Audits and Compliance

**11.1** The Processor shall make available to the Controller all information reasonably necessary to demonstrate compliance with this Agreement and allow for audits conducted by the Controller or an auditor mandated by the Controller, subject to reasonable notice, proportionality, and confidentiality obligations.

## 12. Liability

**12.1** Liability arising under or in connection with this Agreement shall be subject to the limitations and exclusions of liability set out in the Pabau Terms of Use.

## 13. Governing Law and Jurisdiction

**13.1** This Agreement shall be governed by and construed in accordance with the laws of England and Wales.

**13.2** The courts of England and Wales shall have exclusive jurisdiction.

## 14. AssemblyAI

**14.1** Audio recordings for Echo AI transcription are transmitted securely (TLS version 1.2 or higher) and not retained longer than needed for transcription completion. No customer audio is used for AI model training. If AssemblyAI processes data outside the UK (e.g., in the US), such transfers are governed by Standard Contractual Clauses with appropriate supplementary measures.

---

## Annex A — Description of Processing

**Categories of Data Subjects**

Patients, clients, practitioners, clinic staff, and authorised administrative users.

**Categories of Personal Data**

Contact details, appointment data, clinical records, treatment notes, billing information, communications, and other data entered into the Pabau platform by the Controller.

**Special Category Data**

Health data and other special category data as defined by the UK GDPR, as determined and controlled by the Controller.

**Purpose of Processing**

Provision of clinic management, scheduling, billing, communications, and digital record keeping functionality.

**Duration of Processing**

For the duration of the services and any lawful retention period thereafter.

---

## Annex B — Technical and Organisational Measures

The Processor implements and maintains appropriate technical and organisational measures to protect Personal Data, including the following.

### 1. Infrastructure and hosting security

Personal Data is hosted on secure cloud infrastructure using reputable providers such as DigitalOcean and Amazon Web Services. Hosting environments are protected by firewalls, network segmentation, monitoring, and regular system maintenance to reduce the risk of unauthorised access or service disruption.

### 2. Encryption

Personal Data is encrypted in transit using industry-standard Transport Layer Security (TLS version 1.2 or higher). Personal Data is encrypted at rest using industry-standard encryption methods. These measures are designed to protect data from interception or unauthorised disclosure.

Customer data is encrypted at rest using AES-256 encryption. Encryption keys for data at rest are managed securely by Pabau (via cloud providers' managed key infrastructure). Customer-supplied encryption keys are not supported.

### 3. Access controls and authentication

Access to Personal Data is restricted through role based access controls. User authentication controls include strong password requirements, optional two factor authentication, session timeouts, and account lockout protections. Additional security features such as user PIN codes and audit logs are used where applicable.

### 4. Application level security

The Pabau platform includes audit trails, activity logging, and configurable user permissions to support accountability and traceability of access to Personal Data. Customers are provided with security configuration tools and recommendations to support appropriate access management.

### 5. Payment security

Payment card data is processed exclusively through PCI compliant third party payment providers such as Stripe. The Processor does not store full card details within the Pabau platform.

### 6. Backup and recovery

Daily backups of data are performed and stored securely to support restoration in the event of accidental deletion, corruption, or system failure. Backup procedures are designed to support data integrity and availability.

### 7. Monitoring and incident response

The Processor operates defined incident response procedures designed to detect, assess, and respond to security incidents. Monitoring tools and periodic security reviews are used to identify vulnerabilities and reduce risk.

### 8. Organisational measures

Staff with access to Personal Data are subject to confidentiality obligations. Access is limited to those who require it for the performance of their duties. Security practices are reviewed periodically to reflect changes in risk, technology, and regulatory expectations.

---

## Annex C — Approved Sub Processors

Amazon Web Services

DigitalOcean

Stripe

SendGrid

Txtlocal

Telnyx

Twilio

**Signature**

Signed for and on behalf of Hambrand Technology Limited trading as Pabau

Name: Kane Wickson

_____

Title: Chief Operating Officer and Data Protection Officer