**SCHEDULE 1: DATA PROCESSING AGREEMENT**
**Version: October 2024**

This Data Processing Agreement ("DPA") is entered into between **3verest PTY Limited** (the "Data Processor") and the **Client** (the "Data Controller") and forms part of the Agreement between the parties to which this DPA is appended.

In the provision of Cloud Services, the Data Controller provides Personal Data to the Data Processor. This DPA sets out the terms and conditions governing the processing of such Personal Data by the Data Processor, including onward transfers to Sub-Processors, for the purposes of providing the Cloud Services. This DPA is designed to ensure compliance with Australian data protection standards and international regulations relevant to the healthcare industry.

## 1. Definitions

1.1. **"Data Controller"**: The entity which determines the purposes and means of the processing of Personal Data.

1.2. **"Data Processor"**: 3verest PTY Limited, which processes Personal Data on behalf of the Data Controller in connection with the provision of Cloud Services.

1.3. **"Data Protection Laws and Regulations"**: All applicable laws and regulations related to the processing of Personal Data, including but not limited to the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs), the UK General Data Protection Regulation (UK GDPR), the EU General Data Protection Regulation (EU GDPR), and any other relevant data protection laws.

1.4. **"Data Subject"**: An identified or identifiable natural person whose Personal Data is being processed.

1.5. **"Personal Data"**: Any information relating to an identified or identifiable natural person submitted to the Cloud Services by the Data Controller, including data related to healthcare, patient records, and other sensitive information.

1.6. **"Processing"**: Any operation or set of operations performed upon Personal Data, whether or not by automated means, including collection, recording, organisation, storage, adaptation, retrieval, consultation, use, disclosure, and destruction.

## 2. Processing of Personal Data

### 2.1. Roles of the Parties

For the purposes of the Data Protection Laws and Regulations, the Client is the Data Controller, and the Data Processor is the entity processing Personal Data on behalf of the Data Controller. The Data Controller authorises the Data Processor to process Personal Data as necessary to provide the Cloud Services as described in the Agreement and this DPA.

### 2.2. Purpose and Duration of Processing

The Data Processor shall process Personal Data solely for the purpose of providing the Cloud Services in accordance with the documented instructions of the Data Controller. Processing shall continue for the duration of the Agreement, unless otherwise required by applicable law or regulation.

### 2.3. Geographic Scope

The Data Processor and its Sub-Processors may process Personal Data in jurisdictions beyond Australia, the Data Controller's country of establishment. The Data Processor shall ensure that any international transfers of Personal Data comply with applicable data protection requirements, including the Privacy Act 1988 (Cth) and Standard Contractual Clauses (SCCs) or other mechanisms as required for transfers outside Australia, the European Economic Area (EEA), and the United Kingdom.

## 3. Data Processor's Obligations

3.1. **Processing Instructions**
The Data Processor shall process Personal Data only on documented instructions from the Data Controller, as set forth in the Agreement, this DPA, or any applicable Order Form(s). Any additional instructions must be agreed upon in writing. The Data Processor shall not be liable for any claims or damages arising from processing conducted in compliance with the Data Controller's instructions.

3.2. **Security Measures**
The Data Processor shall implement and maintain appropriate technical and organisational measures to protect the security, confidentiality, and integrity of Personal Data, considering the specific requirements of healthcare data. These measures include:

- **Data Encryption**: Personal Data is encrypted both in transit and at rest using industry-standard protocols (e.g., AES-256).
- **Access Management**: Access to Personal Data is restricted to authorised personnel, secured through multi-factor authentication and stringent access control policies.
- **Regular Security Audits**: The Data Processor conducts regular internal and external security audits and vulnerability assessments, with prompt remediation of identified risks.
- **Incident Response Protocols**: The Data Processor maintains incident response protocols tailored to healthcare data breaches, including notification procedures for the Office of the Australian Information Commissioner (OAIC) and other relevant regulatory authorities where applicable.

3.3. **Data Breach Notification**
In the event of a confirmed or suspected data breach affecting Personal Data, the Data Processor shall notify the Data Controller without undue delay, and in any event within 72 hours of becoming aware of the breach. The notification shall include:

- A description of the nature of the breach, including categories and approximate number of Data Subjects and records affected.
- Details of the point of contact for more information.
- The likely consequences of the breach.
- Measures taken or proposed to address the breach and mitigate its adverse effects.

3.4. **Assistance with Data Subject Rights**
The Data Processor shall assist the Data Controller in responding to requests from Data Subjects, including requests for access, correction, and deletion of Personal Data, as well as objections to Processing. Such assistance is provided where the Data Processor has access to relevant Personal Data, and the Data Processor reserves the right to charge reasonable fees if the assistance requires significant effort.

## 4. Sub-Processing

4.1. **Engagement of Sub-Processors**
The Data Processor may engage Sub-Processors to process Personal Data on behalf of the Data Controller, provided that such Sub-Processors are bound by written agreements that impose data protection obligations equivalent to those in this DPA. The Data Processor remains fully liable for the acts and omissions of its Sub-Processors.

4.2. **Notification of Changes to Sub-Processors**
The Data Processor shall provide the Data Controller with notice of any changes to its Sub-Processors, allowing the Data Controller 10 business days to object to the change based on reasonable grounds related to data protection. If an objection is raised, the parties will work together in good faith to find a resolution.

## 5. Warranties

5.1. **Data Processor Warranties**
The Data Processor warrants that it:

- **Compliance with Data Protection Laws**: Will use best efforts to process Personal Data in compliance with its obligations under this DPA and all applicable Data Protection Laws and Regulations, including but not limited to the Privacy Act 1988 (Cth), APPs, UK GDPR, EU GDPR, and other relevant laws.
- **Security Measures**: Has implemented and will maintain appropriate technical and organisational measures designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access, in accordance with industry standards and the specific requirements of the healthcare sector.
- **Employee Training and Confidentiality**: Ensures that personnel authorised to process Personal Data are informed of the confidential nature of the data, receive appropriate training in data protection and privacy, and are bound by confidentiality obligations.
- **Lawful Data Transfers**: Will use best efforts to ensure that any transfer of Personal Data outside Australia, the EEA, or other regions with specific data transfer requirements is conducted in compliance with applicable data transfer mechanisms, including but not limited to Standard Contractual Clauses (SCCs), or other legally recognised mechanisms.

5.2. **Data Controller Warranties**
The Data Controller warrants that it:

- **Lawful Basis for Processing**: Has obtained all necessary consents and permissions from Data Subjects for the Processing of their Personal Data, ensuring that such data is collected and provided to the Data Processor in a manner that complies with all applicable Data Protection Laws and Regulations.
- **Accuracy of Instructions**: Will provide accurate and lawful instructions to the Data Processor regarding the Processing of Personal Data and ensure that any instructions are compliant with the requirements of Data Protection Laws and Regulations.
- **Data Integrity**: Is responsible for the accuracy, quality, and legality of Personal Data provided to the Data Processor, including ensuring that the Personal Data is adequate, relevant, and limited to what is necessary for the purposes for which it is processed.
- **Notification of Changes**: Will promptly notify the Data Processor if there are changes to the scope of Processing, the nature of the data, or any other relevant factor that may impact the data protection obligations under this DPA.

5.3. **Mutual Warranties**
The parties mutually warrant that:

- **Authority to Enter Agreement**: Each party has the full right, power, and authority to enter into this DPA and to perform its obligations under this DPA, and this DPA constitutes a legal, valid, and binding obligation of each party.
- **Non-Infringement**: The execution and performance of this DPA will not cause a breach of any other agreement to which either party is a party or otherwise infringe the rights of any third party.

5.4. **Disclaimer of Other Warranties**
Except as expressly provided in this DPA, the Data Processor makes no other warranties or representations, whether express or implied, including but not limited to warranties of merchantability, fitness for a particular purpose, or non-infringement. The Data Controller acknowledges that the Cloud Services are provided "as-is" and "as available," and the Data Processor does not warrant that the services will be uninterrupted, error-free, or completely secure.

## 6. Audit and Compliance

6.1. **Right to Audit**
The Data Controller may, at its own expense, audit the Data Processor's compliance with this DPA, subject to reasonable notice and during normal business hours, without causing undue disruption to the Data Processor's operations. Audits are limited to one per calendar year unless otherwise required by applicable law.

6.2. **Provision of Audit Reports**
The Data Processor shall provide summary audit reports or certifications demonstrating compliance with applicable data protection standards, such as ISO 27001, upon request from the Data Controller, with sensitive information redacted as necessary.

## 7. Data Transfers

7.1. **International Data Transfers**
For transfers of Personal Data outside Australia, the EEA, or other jurisdictions with specific transfer restrictions, the Data Processor shall use best efforts to implement appropriate safeguards such as Standard Contractual Clauses (SCCs) or other approved mechanisms.

## 8. Return and Deletion of Data

8.1. **Return or Deletion**
Upon termination of the Agreement, or upon written request from the Data Controller, the Data Processor shall securely delete or return all Personal Data, unless retention is required by applicable law.

## 9. Liability and Indemnity

9.1. **Limitation of Liability**
The Data Processor's liability under this DPA is strictly limited as set forth in the Agreement. In no event shall the Data Processor be liable for any indirect, special, incidental, or consequential damages, including loss of profits, loss of data, or any other financial losses arising from or related to the processing of Personal Data, even if the possibility of such damages has been advised.

9.2. **Indemnification**
The Data Controller agrees to indemnify, defend, and hold the Data Processor harmless from any claims, damages, or losses arising from the Data Controller's breach of this DPA, including failure to comply with Data Protection Laws and Regulations.

## 10. Governing Law and Jurisdiction

This DPA is governed by the laws of New South Wales, Australia. The parties agree to submit to the exclusive jurisdiction of the courts of New South Wales for any disputes arising out of or in connection with this DPA.

## Appendix 1: Sub-Processors

| Name | Location | Sub-Processing Activity |
|---|---|---|
| Equinix | Sydney, Australia | Data Centre Facility Management |
| Equinix | Melbourne, Australia | Data Centre Facility Management |