ZANDA GLOBAL DATA PROCESSING AGREEMENT ("DPA")

This Global Data Processing Agreement ("DPA") is an agreement between you and the entity you represent (collectively referred to as "Customer," "you," or "your") and Zanda Health Pty Ltd (“Zanda”, “we”, “us”, or “our”). This DPA supplements the Zanda Platform Terms of Use ("Terms of Use") and governs the Processing of Personal Data by Zanda on behalf of the Customer in connection with the Customer's use of the Services.

The following appendices are attached and are an integral part of this DPA. Each appendix applies as required by the Customer’s local regulations:

- APPENDIX I – EU STANDARD CONTRACTUAL CLAUSES: CONTROLLER TO PROCESSOR: Governs the transfer of Personal Data from the EU to Zanda as a data processor in compliance with EU data protection laws.
- APPENDIX II – UK INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES: Provides additional safeguards and terms for data transfers from the UK to Zanda in compliance with UK data protection laws.
- APPENDIX III – US HIPAA BUSINESS ASSOCIATE AGREEMENT: Outlines Zanda’s obligations as a Business Associate when handling Protected Health Information (PHI) under the US Health Insurance Portability and Accountability Act (HIPAA).

By accessing or using the Services you acknowledge that you have read, understood, and agree to be bound by this DPA. This DPA becomes effective upon your subscription to the Services and remains in effect for the duration of your subscription. All capitalised terms used in this DPA will have the meanings given to them in Section 14 of this DPA.

1. Details of Data Processing

1.1. Scope and Roles

This DPA applies to Processing Customer Data to provide the Services. Zanda acts as the Data Processor on behalf of the Customer, the Data Controller.

1.2. Data Processing Activities

1.2.1. Subject Matter: The subject matter of the Processing under this DPA is the Personal Data entered into, processed by, or transmitted through the Zanda Practice Management Platform by the Customer, its authorised users or patients.

1.2.2. Duration: The Processing of Personal Data shall commence upon the effective date of the Customer's subscription to the Services and shall continue for the duration of the subscription. Processing activities will persist until all Personal Data is deleted or returned in accordance with Section 10 (Termination of the DPA) of this DPA.

1.2.3. Nature of Processing: Zanda will perform various Processing activities necessary to provide the Services, which may include the collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, disclosure by transmission, alignment, combination, restriction, erasure, or destruction of data.

1.2.4. Purpose of Processing: The purpose of the Processing is to deliver the features and functionalities of the Zanda Practice Management Platform to the Customer.

1.2.5. Type of Personal Data: This may include identification data, contact information, demographic data, financial information, health and medical information, and any other Personal Data entered by the Customer or their patients.

1.2.6. Categories of Individual Data: Customer clients, healthcare professionals, administrative personnel, and any other individuals whose Personal Data is inputted into the Services by the Customer or their patients.

2. Documented Instructions

2.1. Providing Instructions

2.1.1. Acknowledgement of Instructions: The parties acknowledge that, under this Data Processing Agreement (DPA), the Customer's instructions for the Processing of Personal Data are communicated through the use of the platform's functionalities and configurations. Actions taken by the Customer and its authorised users within the

Services are deemed as documented instructions for the purposes of this DPA.

2.1.2. Processing in Accordance with Instructions: Zanda commits to Processing Customer Data exclusively in accordance with these instructions. This includes adhering to the configurations set by the Customer within the Services and Processing activities necessary to provide the functionalities requested by the Customer.

2.2. Additional Instructions

Any instructions beyond those specified in Section 2.1 require a prior written agreement between Zanda and the Customer. These may involve data processing activities not part of the Services' standard functionalities. Both parties shall negotiate in good faith to agree upon such additional instructions, documenting them in writing and specifying any extra processing activities, responsibilities, timelines, and associated fees if applicable.

3. Confidentiality

3.1. Data Confidentiality

Zanda shall maintain the confidentiality of Personal Data and shall not disclose it to third parties unless authorised by the Customer, permitted by the Terms of Use or required by law.

3.2. Personnel Confidentiality

All Zanda personnel authorised to process Personal Data are subject to confidentiality obligations, including those required by applicable laws, and receive appropriate training on data protection.

3.3. Government Requests

If a governmental body requests access to Personal Data, Zanda shall notify the Customer unless prohibited by law and shall limit the disclosure to the minimum necessary. In the event of a legally binding request, Zanda will verify the validity of the request, and take reasonable steps to ensure any disclosure complies with applicable data protection laws. Zanda will also

provide the Customer with relevant information about the request and any disclosed data, to the extent legally permissible.

3.4. Duties to Inform

In the event of any third-party request to access Personal Data due to legal processes (e.g., due to bankruptcy or insolvency proceedings) Zanda shall endeavor to inform the Customer in a timely manner.

4. Security of Data Processing

4.1. Technical and Organizational Measures

Zanda shall implement appropriate technical and organisational measures as described in Annex II – Security Standards to ensure a level of security appropriate to the risk, including but not limited to:

- Encryption of Personal Data in transit and at rest.
- Access Controls to limit access to authorised personnel.
- Incident Response Procedures to promptly address security incidents.
- Regular Testing and Auditing of security measures.

4.2. Security Assessments

Zanda shall regularly assess and evaluate the effectiveness of its security measures.

5. Sub-processing

5.1. Authorized Sub-processors

5.1.1. General Authorization: The Customer grants Zanda a broad authorisation to engage Sub-processors for data processing activities concerning Customer Data, as specified in this Section.

5.1.2. Current Sub-processors: You can find an up-to-date list of Sub-processors engaged by Zanda, along with details about their roles and locations, at https://www.zandahealth.com/privacy-policy/ under the section "How your data might be shared." Zanda commits to maintaining and regularly updating this list to reflect any changes in its

Sub-processing activities.

5.2. Notification of New Sub-processors

5.2.1. Advance Notice: Zanda shall provide the Customer with prior notice of any intended addition or replacement of Sub-processors. Notification will be given through an appropriate mechanism, such as in-app or email communication where possible at least 14 days before the new Sub-processor processes any Customer Data.

5.2.2. Objection Rights: If the Customer objects to the engagement of a new Sub-processor on reasonable grounds relating to data protection, the Customer may choose to:

5.2.2.1. Terminate the DPA and Services: Terminate this Agreement requesting the closure of their account and the related Services by providing a written notice as outlined in the section 10.1 Termination by the Customer, subject to any applicable terms in the Terms of Use.

5.2.2.2. Discontinue Specific Functionality: Discontinue the use of the specific functionality or Services that require the use of the new Sub-processor without penalty.

5.3. Emergency Replacement

5.3.1. Immediate Engagement: Notwithstanding the foregoing, Zanda may replace a Sub-processor or engage a new Sub-processor it deems necessary to maintain the immediate security and availability of the Services.

5.3.2. Post-Notification: In such cases, Zanda will notify the Customer of the change as soon as reasonably practicable, and the Customer retains the right to object as per Section 5.2.

6. Individual Requests Concerning Their Personal Data

6.1. Service Controls

6.1.1. Technical and Organizational Measures: Considering the nature of the Processing, Zanda shall provide the Customer with Service Controls that constitute the technical and organisational measures by which Zanda assists the Customer in fulfilling its obligations as a Data

Controller to respond to Individuals requests under applicable Privacy Laws.

6.1.2. Functionality Provided: The Service Controls enable the Customer to manage and process requests related to Individual rights, including but not limited to:

- Access: Facilitating the retrieval of Personal Data pertaining to an Individual.
- Rectification: Allowing the correction of inaccurate or incomplete Personal Data.
- Erasure: Enabling the deletion of Personal Data upon valid request.
- Data Portability: Providing mechanisms to export Personal Data in a structured, commonly used, and machine-readable format.
- Consent Management: Recording, managing, and withdrawing Individuals consent where applicable.

6.2. Direct Requests from Individuals

Referral to Customer: Given Zanda's role as a Data Processor and the nature of the Processing, if an Individual (e.g. patient) submits a request directly to Zanda, Zanda shall promptly notify the Individual that it is not the Data Controller for their Personal Data and advise them to direct their request to the Customer, who is the Data Controller.

6.3. Scope of Assistance

Defined Assistance: Both parties acknowledge that the utilisation of Service Controls, as described in Section 6.1, and the process by which Zanda notifies and guides Individuals to direct their requests to the Customer, as outlined in Section 6.2, define the scope and extent of assistance that Zanda, as a Data Processor, is obligated to provide to the Customer under this DPA and applicable Privacy Laws.

6.4. Inaccurate or Outdated Data

6.4.1. Unlikely Awareness: Considering the nature of the Processing and the systems in place, the Customer agrees that it is unlikely that Zanda

would become aware that Customer Data processed under this DPA is inaccurate or outdated.

6.4.2. Notification of Inaccuracies: Nevertheless, if Zanda becomes aware that any Customer Data is inaccurate, incomplete, or outdated, it shall inform the Customer without undue delay.

6.5. Compliance with Privacy Laws

6.5.1. Customer Responsibility: The Customer is responsible for handling Individual requests in compliance with applicable Privacy Laws, using the tools and functionalities provided by the Service Controls.

6.5.2. Processor Cooperation: Zanda shall, upon the Customer's written request and to the extent legally permitted, provide reasonable assistance to the Customer in responding to Individual requests, in cases where the Customer cannot address the request through the Service Controls. Depending on the extent and complexity of the request, Zanda reserves the right to charge a reasonable fee for such assistance.

7. Personal Data Breach Notification

7.1. Processor Notification

7.1.1. Prompt Notification: Zanda shall promptly inform the Customer of any Personal Data Breach affecting Customer Data after becoming aware of the breach. Notification shall be made without undue delay and, where feasible, no later than 48 hours after identifying the breach.

7.1.2. Method of Notification: Notifications will be sent to the Customer's designated administrators through a communication method chosen by Zanda, which may include email, in-platform notifications, or other direct communication channels.

7.1.3. The notification shall include:

- The nature of the Personal Data Breach.
- The categories and approximate number of Individuals and Personal Data records concerned.
- The likely consequences of the Personal Data Breach.

- Measures taken or proposed to address the Personal Data Breach.

7.2. Processor Assistance

7.2.1. Collaboration and Support: To facilitate the Customer's compliance, Zanda shall cooperate with and assist the Customer by providing relevant information about the Personal Data Breach as described in Section 7.1, to the extent that Zanda is able and permitted to disclose such information under applicable laws.

7.2.2. Extent of Assistance: Both parties acknowledge that the manner in which Zanda collaborates with and assists the Customer, as described in this Section 7, defines the scope and extent of assistance that Zanda, operating as a Data Processor, is obligated to provide under this DPA and applicable Privacy Laws.

8. Certifications and Audits

8.1. Processor Compliance

8.1.1. Provision of Information: In addition to the information detailed in the Annex 1 – Security Standards in this Data Processing Agreement (DPA), upon the Customer's written request and provided there is an active non-disclosure agreement (NDA) between the parties, Zanda commits to making available the following:

8.1.1.1. Audit Reports: A public version of the latest audit reports conducted by independent third-party auditors, verifying the adequacy of Zanda's security measures.

8.1.1.2. Security Certifications: A security certificate issued by an accredited certification body, demonstrating compliance with recognised security standards (e.g., ISO 27001 or equivalent).

8.2. Zanda Initiated Audits

8.2.1. Regular Assessments: Zanda utilizes external auditors to evaluate the effectiveness and adequacy of its technical and organizational security measures.

8.2.2. Audit Intervals: These audits are performed at planned intervals determined by Zanda's risk assessment and appetite, ensuring ongoing compliance and security enhancement.

8.2.3. Independent Auditors: All audits are carried out by independent third-party auditors with expertise in data protection and information security.

8.3. Customer Audit Rights

8.3.1. Right to Audit: In alignment with relevant Privacy Laws, Zanda grants the Customer the right to conduct audits of reasonable duration, focusing on the Processing operations associated with the Services provided under this DPA.

8.3.2. Initiation of Audit:The Customer shall initiate the audit request through a designated channel, providing at least 30 days advanced written notice.The request must include detailed information about the proposed scope, objectives, and duration of the audit to facilitate an efficient process.

8.3.3. Conducting the Audit

8.3.3.1. Collaboration: Both parties commit to collaborative efforts to facilitate the audit in accordance with applicable legal and contractual provisions.

8.3.3.2. Access to Information: Zanda shall provide access to relevant information and personnel necessary to demonstrate compliance with Privacy Laws and this DPA.

8.3.3.3. Confidentiality: All information obtained during the audit shall be treated as confidential, and the Customer shall ensure that any third-party auditors are bound by confidentiality obligations.

8.3.4. Audit Conditions

8.3.4.1. Frequency: Audits may be conducted no more than once per year unless mandated by a Supervisory Authority or in the event of a confirmed Personal Data Breach.

8.3.4.2. Costs: The audit shall be conducted at the Customer's expense, including any costs incurred by Zanda to support the audit activities.

8.3.4.3. Minimising Disruption: Audits shall be conducted during normal business hours and in a manner that minimises disruption to Zanda's operations.

8.3.5. Limitations

Customer audit rights are exercised only to the extent that the information provided in this DPA, particularly under Section 8.1, does not already offer the required information and assurance. If the requested audit scope is covered by an audit report or certification provided under Section 8.1, the Customer shall accept these findings in place of conducting a separate audit. Audit requests may be denied if they pose a security or commercial risk, or if we reasonably determine the request to be excessive or unreasonable.

8.4. Customer Compliance Assistance

8.4.1. Security Questionnaires: Zanda assists customers by providing the documentation specified in Section 8.1 and the information available on our security page to support the completion of security questionnaires. Any requests for additional information beyond these resources fall outside our standard support scope and will be evaluated on a case-by-case basis..

8.4.2. Assistance with Data Protection Impact Assessments (DPIAs): Zanda will assist Customers with DPIAs as required under applicable data protection laws. Assistance beyond standard obligations may incur additional fees, subject to prior written agreement.

8.4.3. Scope of Assistance: Assistance is limited to information in Zanda's possession and does not extend to information held by third parties or the Customer's internal processes. Zanda's support does not include legal or regulatory advice but focuses on providing factual information regarding its data protection measures.

9. Cross-border Transfer Mechanisms

9.1. Jurisdiction-Specific Requirements

9.1.1. Non-Jurisdictional Approach: This Clause 9 is designed to be applicable regardless of the specific jurisdictions involved in the Restricted Transfer, acknowledging that various Privacy Laws may impose different requirements for cross-border data transfers.

9.1.2. Supplemental Measures: Where specific jurisdictions require additional measures or contractual terms to legitimize Restricted Transfers, the parties agree to cooperate in good faith to incorporate such measures into this DPA as necessary, either through appendices, addenda, or updated terms.

9.2. Permitted Transfer Mechanisms

9.2.1. Appropriate Safeguards: The parties agree that any Restricted Transfer of Personal Data shall be undertaken using one or more of the following permitted transfer mechanisms ("Permitted Transfer Mechanisms") to ensure an adequate level of protection for the Personal Data:

- Adequacy Decisions or Recognitions: Transfers to jurisdictions that have been officially recognized by relevant authorities as providing an adequate level of data protection.
- Standard Contractual Clauses: Implementation of legally enforceable agreements containing standard data protection clauses or other contractual clauses that impose data protection obligations equivalent to those under applicable Privacy Laws.
- Binding Corporate Rules: Adoption of Binding Corporate Rules ("BCRs") approved by relevant authorities, applicable to intra-group transfers within multinational organizations, ensuring consistent data protection practices.
- Approved Codes of Conduct or Certification Mechanisms: Adherence to an approved code of conduct or certification mechanism that includes binding and enforceable commitments to apply appropriate safeguards.
- Explicit Consent: Obtaining the explicit consent of the Data Subject for the specific transfer, after being informed of the

potential risks due to the absence of an adequacy decision and appropriate safeguards.

- Derogations for Specific Situations: Transfers necessary for the performance of a contract between the Data Subject and the Customer, implementation of pre-contractual measures at the Data Subject's request, or other specific situations recognized under applicable Privacy Laws.

10. Account Termination

10.1. Termination by the Customer

The Customer may terminate this Agreement requesting the closure of their account at any time. To initiate termination, the Customer must:

- Send a written notice to Zanda at support@zandahealth.com from the email address associated with their account; or
- Use the in-app cancellation option provided within the Services.

For security and account integrity, termination requests will only be processed if submitted through these methods.

Effective Date of Termination: Your Account termination will become effective as soon as we send you a confirmation notice, which we will issue once the following steps are complete:

- Received your termination request, either through the in-app closure option or by email from the address associated with your Account.
- Verified the request against our security protocols to confirm its authenticity.
- All outstanding fees or charges owed to Zanda have been paid in full.

After these conditions are met, we will promptly process the termination and provide you with a confirmation notice.

Cessation of Access: Upon the effective date of termination, the Customer's access to the Services will be discontinued.

10.2. Termination by Zanda

Zanda may terminate this Agreement and suspend or discontinue the Services immediately upon written notice to the Customer if:

- The Customer breaches any material term of this Agreement or the Zanda's Terms of Use and fails to remedy the breach after receiving notice of the breach.
- Required to do so by law or in response to a legal process.
- Continuing to provide the Services could create substantial economic or technical burdens or security or privacy risks for Zanda.
- Fail to pay any fees or charges owed to Zanda.

Notice of Termination: Zanda will provide written notice to the Customer's registered email address detailing the reasons for termination when feasible.

10.3. Customer Data Return and Deletion

10.3.1. Data Portability and Export Responsibility

- Customer's Responsibility: The Customer is solely responsible for exporting or backing up Customer Data they wish to retain prior to the effective date of termination.
- Assistance with Data Retrieval: Both parties acknowledge that the "Service Controls" provided by Zanda constitute the means by which Zanda will assist the Customer in retrieving their Customer Data. These controls define the scope and extent of assistance that Zanda, acting as a Data Processor, is obligated to provide under this DPA and applicable privacy laws.

10.3.2. Deletion of Customer Data

- Permanent Deletion: After the Effective Date of Termination, Zanda may permanently and irreversibly delete any remaining Customer Data data without further notice, except where legal obligations require otherwise. This deletion process is irreversible, and no account reactivation, reinstatement of Services, or restoration of data will be possible after this period.

- Compliance with Privacy Laws: Zanda will carry out the deletion of Customer Data in compliance with applicable data protection laws, ensuring that all personal data is securely and permanently erased.

11. Compliance with Privacy Laws

11.1. Mutual Assistance

The parties shall cooperate and assist each other in complying with their obligations under applicable Privacy Laws.

11.2. Changes in Law and Amendments

If changes in Privacy Laws require modifications to this DPA, the parties shall negotiate in good faith to amend the DPA accordingly. We may update or modify this DPA from time to time. Any amendments will be effective upon posting the revised DPA within the Services or on our website. By continuing to access or use the Services after any such amendments become effective, you agree to be bound by the updated DPA.

12. General Terms

12.1. Order of Precedence

In the event of a conflict between this DPA and other agreements, the terms of this DPA shall prevail with regard to data protection matters.

12.2. Severability

If any provision of this DPA is held invalid or unenforceable, the remaining provisions shall remain in full force and effect.

12.3. Entire Agreement

This Global Data Processing Agreement ("DPA"), including all its addenda and annexes, supplements the Terms of Use specifically concerning data protection matters. Together, the DPA and the Terms of Use constitute the entire agreement between the parties regarding data protection.

13. Governing Law and Jurisdiction

Except where mandated by applicable Privacy Laws, this DPA shall be governed by and construed in accordance with the laws of the State of Victoria, Australia. Any disputes arising out of or in connection with this DPA shall be subject to the exclusive jurisdiction of the courts of the State of Victoria, Australia.

14. Definitions

- **"Adequacy Decision"** means a decision by a Supervisory Authority or other competent body that a country or territory ensures an adequate level of protection for Personal Data.
- "**Customer"** An individual or entity that subscribes to the Service.
- "**Customer Data**" refers to all data, including all categories of Personal Data, uploaded or inputted by the Customer into the Service.
- **"Data Controller"** means the entity that determines the purposes and means of the Processing of Personal Data; in this context, the Customer.
- **"Data Processor"** means the entity that Processes Personal Data on behalf of the Data Controller; in this context, Zanda.
- **"Individuals"** means identified or identifiable natural persons whose Personal Data is processed.
- **"Personal Data"** refers to any information relating to an identified or identifiable natural person, as defined under applicable Privacy Laws.
- **"Personal Data Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.
- **"Privacy Laws"** refers to all applicable laws and regulations relating to the processing of Personal Data, including but not limited to the Australian Privacy Act 1988 (Cth), the New Zealand Privacy Act 2020, the EU General Data Protection Regulation 2016/679 ("EU GDPR"), the UK Data Protection Act 2018 ("UK GDPR"), the California Consumer Privacy Act of 2018 ("CCPA"), the Personal Information Protection and Electronic Documents Act ("PIPEDA"), and South Africa's Protection of Personal Information Act ("POPIA").
- "**Process," "Processing," or "Processed"** means any operation or set of operations performed on Personal Data, such as collection, recording,

organisation, structuring, storage, adaptation, retrieval, consultation, use, disclosure, dissemination, alignment, restriction, erasure, or destruction.

- **"Restricted Transfer"** refers to any transfer of Personal Data that is subject to cross-border transfer restrictions under applicable Privacy Laws.
- **"Services"** refers to the features and functionalities provided by Zanda to the Customer as part of the Zanda Practice Management platform subscription.
- **"Service Controls**" refers to the functionalities within the Services designed to assist the Customer in upholding Individuals' privacy rights, including access, deletion, and porting of Personal Data, as well as recording individual consent.
- **"Standard Contractual Clauses"** means the contractual clauses adopted by the European Commission or other relevant authority for the transfer of Personal Data to third countries.
- **"Sub-processor"** means any third party engaged by Zanda to Process Personal Data on behalf of the Customer.
- **"Supervisory Authority**" means an independent public authority established pursuant to applicable Privacy Laws responsible for monitoring and enforcing compliance.
- **"User**" An individual authorized by the Customer to use the Service for uploading or inputting client or patient information.

APPENDIX I – EU STANDARD CONTRACTUAL CLAUSES - CONTROLLER TO PROCESSOR

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ([1]) for the transfer of data to a third country.

[1]free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content

or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter ‘personal data breach’). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of

pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences

(hereinafter ‘sensitive data’), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([2]) (in the same country as the data importer or in another third country, hereinafter ‘onward transfer’) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter’s request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union’s internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 14 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([3]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information,

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the

data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([4]);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations

under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts

ANNEX I - A. LIST OF PARTIES

Data exporter(s):

Name:
Customer (as defined in Section 14, "Definitions," of the Global Data Processing Agreement ("DPA"))

Address:
Customer's registered address as specified in their account details.

Activities relevant to the data transferred under these Clauses:
Refer to Section 1, "Details of Data Processing," of the DPA.

Contact person's name, position and contact details:
As listed in the Customer's account profile, including name, position, and contact information.

Signature:
By using the Services, the Customer affirms they have read, understood, and accepted the terms of this DPA.

Effective Date: This agreement takes effect starting from the subscription start date outlined in the customer's account profile details.

Role: Controller/Covered Entity

Data importer(s):

Name:
Zanda Health Pty Ltd.

Address:
1006a Eyre Street, Ballarat Central
VIC 3350 - AUSTRALIA

Activities relevant to the data transferred under these Clauses:
Refer to Section 1, "Details of Data Processing," of the DPA.

Contact person's name, position and contact details:

Signature:
Tercyus Ribeiro
Data Protection Officer
tercyus.ribeiro@zandahealth.com

Effective Date: This agreement takes effect starting from the subscription start date outlined in the customer's account profile details.

Role: Processor/Business Associate

ANNEX I - B. DESCRIPTION OF TRANSFER

Refer to Section 1, "Details of Data Processing," in the Global Data Processing Agreement ("DPA") outlined above.

ANNEX I - C. COMPETENT SUPERVISORY AUTHORITY

Ireland - Data Protection Commission (DPC) - Reference: DPC-13-0812-101958-bd732

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Zanda implements the following technical and organisational measures to protect Personal Data:

1. Access Control
    - System Access Control: Access to systems is restricted through strong authentication mechanisms, including unique user IDs, complex passwords, and two-factor authentication (2FA). Access rights are granted on a least-privilege basis and reviewed regularly.
    - Data Access Control: Only authorized personnel with a legitimate business need can access Personal Data. Access logs are maintained and monitored for unauthorized activities.

2. Data Transmission Control
    - Encryption in Transit: All data transmitted between users and Zanda servers is encrypted using industry-standard Transport Layer Security (TLS) protocols to protect against interception and eavesdropping.
    - Network Security: Firewalls and intrusion detection systems are employed to monitor and protect network traffic from malicious activities.

3. Data Storage Control

- Encryption at Rest: Personal Data stored on servers is encrypted using strong encryption algorithms to safeguard against unauthorized access in case of a security breach.
- Secure Storage Solutions: Data is stored in secure environments with redundancy and backup capabilities to prevent data loss.

4. Input Control
    - Logging and Monitoring: System activities, including data entry, modification, and deletion, are logged to create an audit trail. Logs are regularly reviewed for suspicious activities.
    - Access Logging: Detailed logs of user access to Personal Data are maintained to monitor and audit data access patterns.

5. Sub-processor Management
    - Sub-processor Management: Third-party service providers (sub-processors) are carefully evaluated for security compliance. Contracts with sub-processors include data protection obligations equivalent to those in the Data Processing Agreement.

6. Training and Awareness
    - Employee Training and Awareness: Employees receive regular training on data protection laws, security policies, and privacy practices to ensure compliance and awareness.

7. Availability Control
    - Redundancy and Backup Systems: Critical systems and data have redundancy solutions and regular backups to ensure availability and quick recovery in case of system failures.
    - Disaster Recovery and Business Continuity Plans: Comprehensive plans are in place to maintain service continuity during unforeseen events, tested and updated regularly.

8. Separation Control
    - Data Segregation: Personal Data is logically segregated to prevent accidental mixing with other data. Multi-tenancy systems ensure that each customer's data remains isolated.

- Environment Separation: Development, testing, and production environments are separated to prevent unauthorized access to live Personal Data during software development and testing.

9. Pseudonymisation and Encryption
    - Data Minimization: Only the minimum necessary Personal Data is collected and processed for the intended purpose.
    - Pseudonymisation Techniques: Where appropriate, data is pseudonymised to reduce the risk associated with data processing.

10. Integrity and Confidentiality
    - Secure Development Practices: Software is developed following secure coding standards to prevent vulnerabilities.

11. Incident Response Management
    - Incident Detection and Response: Procedures are established to promptly detect, investigate, and respond to security incidents and Personal Data breaches.
    - Notification Procedures: In the event of a Personal Data breach, Zanda will notify the Customer without undue delay, in accordance with the Data Processing Agreement.

12. Regular Testing and Evaluation
    - Security Assessments: Regular vulnerability scans, penetration testing, and security assessments are conducted to identify and mitigate risks.
    - Audit and Compliance Checks: Internal and external audits are performed to ensure ongoing compliance with security policies and legal requirements.

13. Organisational Measures
    - Security Policies and Procedures: Comprehensive security policies are documented, implemented, and reviewed regularly to reflect changes in regulations and technology.
    - Confidentiality Obligations: All personnel authorized to process Personal Data are subject to confidentiality obligations, including statutory confidentiality requirements.

14. Data Protection by Design and Default

- Privacy Impact Assessments: Data protection impact assessments are conducted for new processing activities that may pose high risks to individuals' rights and freedoms.
- Default Settings: Systems are configured by default to provide the highest level of privacy protection.

15. Data Deletion and Return
    - Secure Deletion Practices: Procedures are in place to securely delete or anonymize Personal Data when it is no longer needed, using methods that prevent data recovery.
    - Data Portability: Upon request, Personal Data can be returned to the Customer in a structured, commonly used, and machine-readable format.

16. Compliance with Laws and Regulations
    - Regulatory Monitoring: Zanda actively monitors changes in data protection laws and updates its practices accordingly.
    - Legal Compliance Checks: Regular reviews are conducted to ensure compliance with applicable legal obligations.

These technical and organisational measures are designed to ensure a level of security appropriate to the risk and to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access.

ANNEX III - LIST OF SUB-PROCESSORS

The controller has approved the use of the sub-processors listed in Section 5, "Sub-processing," of the Global Data Processing Agreement (DPA).

APPENDIX II - UK INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

- Refer to Annex I, A. List of parties

Table 2: Selected SCCs, Modules and Selected Clauses

The version of the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

- As set out in Clause 9 Use of sub-processors of the approved EU SCCs

Table 3: Appendix Information

“Appendix Information” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

- Annex 1A: List of Parties
- Annex 1B: Description of Transfer
- Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data
- Annex III: List of Sub processors

Table 4: Ending this Addendum when the Approved Addendum Changes

This addendum can be ended in order to incorporate an approved addendum changes by both parts.

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.

Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from

it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:
    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCC;

    b. In Clause 2, delete the words:
        "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

    c. Clause 6 (Description of the transfer(s)) is replaced with:
        "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

    d. Clause 8.7(i) of Module 1 is replaced with:
        "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

    e. Clause 8.8(i) of Modules 2 and 3 is replaced with:
        "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

    f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of

natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:
    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;

    The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:
    a. its direct costs of performing its obligations under the Addendum; and/or
    b. its risk under the Addendum,

    and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Alternative Part 2 Mandatory Clauses:

Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with

s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

APPENDIX III - US HIPAA BUSINESS ASSOCIATE AGREEMENT (BAA)

This Business Associate Agreement (BAA) appendix, referencing Annex I, Section A: List of Parties, is effective as of the subscription start date specified in the customer's account details, establishing the Agreement's Effective Date.

This agreement is intended by both parties as a final, exclusive, and complete expression of the terms contained in the agreement and supersedes all prior understandings and agreements (either written or oral) between the two parties with regard to the subject matter contained. The parties agree as follows:

1. **Definitions**

   Catch-all definition: The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

   Specific definitions:

   a. Business Associate. "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean Business Associate.

   b. Covered Entity. "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean Covered Entity.

c. HIPAA Rules. “HIPPA Rules” shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

2. Obligations and Activities of Business Associate

Business Associate agrees to:

a. Not use or disclose protected health information other than as permitted or required by the Agreement or as required by law;

b. Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement;

c. Report to covered entity any use or disclosure of protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware;

d. In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information;

e. Make available protected health information in a designated record set to the Covered Entity as necessary to satisfy covered entity’s obligations under 45 CFR 164.524;

f. Make any amendment(s) to protected health information in a designated record set as directed or agreed to by the covered entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy covered entity’s obligations under 45 CFR 164.526;

g. Maintain and make available the information required to provide an accounting of disclosures to the Covered Entity as necessary to satisfy covered entity’s obligations under 45 CFR 164.528;

h. To the extent the business associate is to carry out one or more of covered entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the covered entity in the performance of such obligation(s); and

i. Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

3. Permitted Uses and Disclosures by Business Associate

a. Business associate may only use or disclose protected health information as necessary to perform the services set forth in Service Agreement.

b. Business associate may use or disclose protected health information as required by law.

c. Business associate agrees to make uses and disclosures and requests for protected health information consistent with covered entity's minimum necessary policies and procedures.

d. Business associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by covered entity except for the specific uses and disclosures set forth below.

e. Business associate may use protected health information for the proper management and administration of the business associate or to carry out the legal responsibilities of the business associate.

f. Business associate may disclose protected health information for the proper management and administration of business associate or to carry out the legal responsibilities of the business associate, provided the disclosures are required by law, or business associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

g. Business associate may provide data aggregation services related to the health care operations of the covered entity.

4. **Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions**

   a. Covered entity shall notify business associate of any limitation(s) in the notice of privacy practices of covered entity under 45 CFR 164.520, to the extent that such limitation may affect business associate's use or disclosure of protected health information.

   b. Covered entity shall notify business associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her protected health information, to the extent that such changes may affect business associate's use or disclosure of protected health information.

   c. Covered entity shall notify business associate of any restriction on the use or disclosure of protected health information that covered entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect business associate's use or disclosure of protected health information.

5. Permissible Requests by Covered Entity

Covered entity shall not request business associate to use or disclose protected health information in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by covered entity except as described above in Section 3 of the Agreement.

6. Term and Termination

   a. Term. The Term of this Agreement shall be effective as of the Effective Date of the Agreement, and shall continue until terminated by either party.

   b. Termination for Cause. Business associate authorizes termination of this Agreement by covered entity, if the covered entity determines the business associate has violated a material term of the Agreement [and the business associate has not cured the breach or ended the violation within the time specified by the covered entity].

c. Obligations of Business Associate Upon Termination.
Upon termination of this Agreement for any reason, business associate, with respect to protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, shall:

1. Retain only that protected health information which is necessary for business associate to continue its proper management and administration or to carry out its legal responsibilities;

2. Return to covered entity [or, if agreed to by covered entity, destroy] the remaining protected health information that the business associate still maintains in any form;

3. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, other than as provided for in this Section, for as long as business associate retains the protected health information;

4. Not use or disclose the protected health information retained by business associate other than for the purposes for which such protected health information was retained and subject to the same conditions set out in Section 3 of the Agreement which applied prior to termination; and

5. Return to covered entity [or, if agreed to by covered entity, destroy] the protected health information retained by business associate when it is no longer needed by the business associate for proper management and administration or to carry out its legal responsibilities.

d. Survival. The obligations of the business associate under this Section shall survive the termination of this Agreement.