PANASEER - DATA PROCESSING AGREEMENT

This Data Processing Agreement (the "**DPA**") is entered into by and between Panaseer Limited, a company registered in England and Wales with company number 09098199 whose registered office is Ashcombe Court, Woolsack Way, Godalming, Surrey, GU7 1LQ (or its U.S. subsidiary Panaseer Inc), (both "**Panaseer**"), and the entity described as "Customer" in the Order or a Statement of Work, as applicable (the "**Customer**").

Panaseer and Customer are hereinafter individually referred to as a **"Party"** and jointly, the **"Parties"**.

1. Background and Definitions

1.1 This DPA has been made in connection with and is a part of the Subscription Terms **("Agreement")** entered into between Panaseer and the Customer concerning Panaseer's Software and Professional Services as described in the Agreement and the applicable Order or Statement of Work.

1.2 This DPA shall enter into effect as of the Effective Date of the Agreement.

1.3 The Agreement governs ordinary matters relating to the Software and Professional Services (if any) provided by Panaseer to the Customer and this DPA governs associated transfers of personal data. To the extent relating to the scope of this DPA on data protection, this DPA prevails in case of any discrepancies between this DPA and all other agreements, including the Agreement and its other appendices, made between the Parties.

1.4 Any term beginning with a capital letter and not defined herein shall have the meaning determined under the Agreement.

1.5 Any reference to this DPA is also a reference to its appendices.

1.6 The Agreement remains confidential between the Parties to the effect that any sub-processors may be informed of the contents of this DPA only to the extent necessary.

1.7 **Definitions**

Appropriate Safeguards	means such legally enforceable mechanism(s) for transfers of Personal Data as may be permitted under Data Protection Laws from time to time;
Data Protection Laws	means all applicable laws, regulations, and standards regarding data protection, privacy, and the processing of personal data as applicable and binding on the Parties and/or the Services including but not limited to: (i) Regulation 2016/679 of the European Parliament and of the Council 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) (the "**EU GDPR**"); (ii) the Data Protection Act 2018 and EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (and regulations made thereunder) (the "**UK GDPR**"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); (iv) the California Consumer Privacy Act 2018, as amended by the California

Privacy Rights Act 2020; and (iv) any and all applicable national data protection laws made under, pursuant to, or that apply in conjunction with, any of the above; in each case as may be amended or superseded from time to time;

CCPA	means the California Consumer Privacy Act of 2018, together with all regulations implementing or supplementing the same, to the extent applicable to Panaseer in its performance of the Services. Only to the extent Panaseer processes personal information of Californian residents that Customer provides or makes available to Panaseer in connection with the Services, the CCPA Addendum (Appendix C) will apply.
EU SCCs	means the Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679, adopted by the European Commission decision (EU) 2021/914 of 4 June 2021;
Protected Data	means personal data received from or on behalf of the Customer to the extent that it is processed by Panaseer on Customer's behalf in connection with the performance of Panaseer's obligations under the Agreement;
Services	means the Software and Professional Services (if any) to be provided under the Agreement.
UK SCCs	means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK ICO under S119A(1) Data Protection Act 2018 and in force March 21, 2022.

2. Personal Data and data processing activities

2.1 This DPA defines and governs the personal data, the data subjects, the purposes and the data processing activities that will be carried out by the Parties while performing the Agreement and other matters and obligations relating to the processing, as defined and stated in Annex 2 hereto. The Annexes and Appendices to this DPA form part of both Parties' documentation obligations under Data Protection Laws and must always reflect the actual circumstances.

2.2 The Customer warrants and undertakes that the personal data has been collected, processed and transferred in accordance with applicable Data Protection Laws, including but not limited to the legal grounds for processing and the requirement to provide data subjects with certain information.

3. Roles and instructions

3.1 Customer and Panaseer acknowledge that for the purpose of Data Protection Laws, where the Customer uses the Services and makes decisions about the personal data being processed via the Services, Customer is controller and Panaseer is processor. The Customer decides for which purposes and how Panaseer may process the personal data.

3.2 Panaseer may and shall process the personal data only pursuant to documented instructions from the Customer as set out in **Annexes 1 and 2** and **Appendices A, B and C**, or other written instructions unless required to do so by Data Protection Laws to which Panaseer is subject. In such a case, Panaseer must inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

3.3 Customer retains control of the personal data and shall, at all times, comply with applicable Data Protection Laws, including providing any required notices and obtaining any required consents, and for the processing instructions it gives to Panaseer. Customer shall ensure all instructions given by it to Panaseer in respect of Protected Data (shall at all times be in accordance with all

Data Protection Laws. Nothing in the Agreement or this DPA relieves Customer of any responsibilities or liabilities under any Data Protection Laws.

3.4 Panaseer must delete and/or dispose of personal data in all systems and files only upon instructions of the Customer.

4. Confidentiality

4.1 The personal data provided to Panaseer by the Customer or otherwise obtained by Panaseer in the course of carrying out the Services is confidential.

4.2 Panaseer must ensure that only employees and other individuals who, at any given time, are required to process the personal data as part of their job have been authorised to do so.

4.3 Panaseer must further ensure that the individuals authorised to process the Customer's personal data have undertaken a duty of confidentiality for all personal data to which they have access or that they are subject to an appropriate statutory duty of confidentiality.

5. Supporting the Rights of the Data Subjects

Considering the nature of processing and the information available to Panaseer, Panaseer shall implement appropriate technical and organisational measures to assist the Customer in the fulfilment of the Customer's legal obligations under Chapter III (Rights of Data Subjects) of the EU GDPR.

6. Security

6.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity of the rights and freedom of natural persons, Panaseer shall implement appropriate technical and organisational measures to ensure a level of security appropriate for the risk, in particular the risk of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to the personal data transmitted, stored or otherwise processed.

7. International Transfers of Personal Data

7.1 The Customer agrees that Panaseer may transfer Protected Data to countries outside the EEA, the United Kingdom or to any international organisation(s) (an **International Recipient**), provided all transfers by Panaseer of Protected Data to an International Recipient shall (to the extent required under Data Protection Laws) be effected by way of Appropriate Safeguards and in accordance with Data Protection Laws. The provisions of this Agreement shall constitute the Customer's instructions with respect to transfers in accordance with Section 3.

7.2 If Customer transfers personal data to Panaseer from the European Economic Area (EEA), Switzerland, or the United Kingdom (UK), the Parties will apply one of the following to the extent an Appropriate Safeguard is legally required in descending order of preference, such that the item highest on the list that is applicable and available will automatically apply during the term of this DPA: (i) a valid finding Adequacy Decision; (ii) any mechanism, derogation, exemption, or exception that the Parties are able to invoke, such as the consent of the relevant data subjects or a derogation under Article 49 of the EU GDPR; or (iii) the applicable EU SCCs and/or UK SCCs pursuant to Appendices A and B. Nothing in the interpretations of this DPA is intended to conflict with either Party's rights or responsibilities under the EU SCCs or UK SCCs and, in the event of any such conflict, the EU SCCs or UK SCCs shall prevail, as applicable. To the extent a transfer mechanism other than the foregoing becomes reasonably available to the Parties after the effective date of this DPA, the Parties will consult with each other in good faith on whether to rely on such transfer mechanism in lieu of the applicable EU SCCs or UK SCCs.

7.3 Without prejudice to the generality of the foregoing, Customer agrees to the transfer of personal data to sub-processors outside of the UK or EEA pursuant to Section 8 or as otherwise notified to Customer by Panaseer pursuant to Section 8 below.

8. Sub-processors

8.1 Subject this section 8, Panaseer has the Customer's general authorisation for the engagement of sub-processors a list of which (the "**Sub-processor List**") is kept in the trust centre section on the Panaseer's website at https://panaseer.com/sub-processors/ ("**Website**"). Panaseer shall ensure that the Sub-processor List is kept current and that any changes to the Sub-processor List are reflected on the Website.

8.2 Panaseer shall inform the Customer about any intended changes to the Sub-processor List reasonably in advance and by giving the Customer sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). If the Customer (acting reasonably) does not approve of a new sub-processor, the Customer may, within 7 (seven) days from the notification to the Customer, request that Panaseer move the Protected Data to another sub-processor by email to DPO@Panaseer.com. If a request is received from Customer within the time frame, Panaseer shall, within a reasonable period of time following receipt of such request, use all reasonable endeavours to ensure that the relevant sub-processor does not process any further Protected Data, and help identify an alternative. If such a request is not received within this time frame, the new sub-processor shall be deemed to have been approved.

8.3 Further, it is a condition for the use of the sub-processor(s) that Panaseer enters into a written agreement with the sub-processor stating the sub-processor's duty to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of applicable Data Protection Laws.

9. Assistance to the Customer

9.1 Taking into account the nature of processing and the information available to Panaseer, at Customer's cost and expense, Panaseer will assist the Customer in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the EU GDPR, i.e. with regard to security measures, notification of supervisory authorities, notification of individuals, preparation of data protection impact assessments and prior consultation with supervisory authorities.

10. Personal Data Breaches

10.1 In case of a Personal Data Breach relating to the Personal Data, Panaseer shall notify the Customer without undue delay of when Panaseer is made aware of the Personal Data Breach.

10.2 Taking into account the nature of processing as well as the information available to Panaseer, following a personal data breach at Panaseer, Panaseer shall assist the Customer in ensuring compliance with the Customer's legal obligations in connection with the notification of personal data breaches to supervisory authorities and to data subjects.

10.3 Further, following a personal data breach at Panaseer, taking into account the nature of processing as well as to the extent the information is available to Panaseer, Panaseer must use its best efforts to provide the Customer with the information stated in the EU GDPR Article 33 without undue delay, to enable the Customer to comply with any statutory obligations.

10.4 If and to the extent that it is not possible to immediately provide the information mentioned under clauses 10.1 - 10.3, the information can be provided gradually but no later than 72 hours from when Panaseer was made aware of the personal data breach.

11. Demonstration of compliance and audits

11.1 Panaseer must upon written request make available to the Customer reasonable information necessary to demonstrate its compliance with the obligations stipulated in this DPA and applicable Data Protection Laws.

11.2 Panaseer shall, at Customer's expense, allow for and contribute to audits, including inspections, conducted by the Customer, auditors mandated by the Customer, or public authorities in competent jurisdictions. The auditor in question must be subject to confidentiality, either contractually or by law.

11.3 The above clauses 11.1 and 11.2 shall not be applicable if Panaseer can present an audit report produced by an external qualified auditor and no older than 12 months without any material remarks regarding compliance with Data Protection Law and the compliance with this DPA.

12. Information

12.1 Panaseer shall immediately inform the Customer if, in its opinion, an instruction infringes any applicable Data Protection Laws.

12.2 To the extent relevant, the Customer must inform Panaseer of any legislation other than the EU or UK GDPR, as for example any special, local requirements for the storage of Personal Data in the country of the Customer. If such special legislation flows down and imposes additional obligations on Panaseer beyond the EU and UK GDPR, the Parties must discuss the additionally required adaption to systems and processes and the payment for any such adaption.

13. Liability

13.1 To the maximum extent allowed by applicable laws, the Parties' liabilities arising out of or in connection with this DPA, whether in contract, tort or under any other theory of liability, will be subject to any aggregate limitation of liability and any exclusions of damages set forth in the Agreement, and any reference to the liability of the Parties shall mean the aggregate liability under the Agreement and this DPA together.

13.2 Panaseer will not be liable for any claim brought by a data subject arising from any action by Panaseer to the extent that such action resulted directly from the Customer's instructions. In such case, the Customer shall indemnify, keep indemnified and defend at its own expense Panaseer against all associated costs, claims, damages or expenses incurred by Panaseer.

13.3 When acting as separate controllers (or where the parties are deemed to be joint controllers) of any Protected Data hereunder, each Party shall only be liable for its own breach of the applicable Data Protection Laws or of this DPA and shall not be jointly and/or severally liable with the other Party for the other Party's breach. Each Party shall on their own be liable for any administrative fines that a supervising authority may impose due to their processing.

14. Severability

14.1 If any of the clauses of this DPA is held invalid, this shall not affect the validity of the remaining DPA.

15. Term and termination

15.1 This DPA shall remain in force for as long as the duration of the Agreement or longer, if terms in the Agreement, this DPA or requirements set out in applicable legislation require so.

15.2 This DPA shall terminate without notice at the time of termination/expiry of the Agreement.

15.3 This DPA applies to all processing of personal data carried out by Panaseer in connection with the provision of the Services and to all personal data held by Panaseer whether held on the date of this DPA or held or received after its expiry or termination. Hence, this DPA, including relevant provisions of the Agreement, will survive for as long as Panaseer processes personal data, also if such processing takes place after termination of this DPA.

15.4 After the end of the provision of the Services and at the termination of this DPA (whichever time is the latest), Panaseer shall, at the discretion of the Customer, delete or return all existing copies of the personal data and delete all existing copies of the personal data processed on behalf of the Customer except for any personal data that Panaseer may be obligated to store according to mandatory laws (as applicable).

15.2 This clause 15 and the relevant references will survive any termination of this DPA.

16. Governing law and venue

16.1 This DPA and all non-contractual or other obligations arising out of or in connection with it are subject to the governing law and jurisdiction provisions of the Agreement, except with respect to (i) the EU SCCs, which shall be governed by the law of Ireland, and (ii) the UK SCCs, which shall be governed by the laws of England and Wales.

17. Appendices

17.1 The following Appendices to this DPA constitute an integral part of the DPA:

Annex 1: Information about the processing operations
Annex 2: Minimum security requirements
Appendix A: EU SCCs
Appendix B: UK SCCs
Appendix C: CCPA Addendum

18. Signatures

18.1 This DPA is effective and deemed agreed on signature of the Agreement.

ANNEX 1
Information about the processing operations

Data subjects

Panaseer processes personal data about the following categories of data subjects for the Customer:

- Customer's employees, contractors or similar with access to Panaseer's Software.

Categories of personal data

Panaseer processes the following **general categories** of personal data about the categories of data subjects below on behalf of the Customer:

- email, first name and last name of data subjects, IP address.

Special categories of personal data

Panaseer processes the following **special categories** of personal data about the categories of data subjects above on behalf of the Customer:

- None.

Purpose

Panaseer's processing of personal data for the Customer is carried out for the following purpose:

- For the purposes of undertaking its obligations and exercising its rights in connection with the Customer's use of the Software, and the provision of the Professional Services:
    - For Customer to be able to use the Software which is owned and managed by Panaseer.
    - For Panaseer to be able offer support and Professional Services to the Customer.

Data Processing Activities/nature of processing operation

Panaseer's processing of personal data for the Customer is carried out through the following activities:

- Performance of the Services described in the Agreement, including hosting and data storage, Software updates and maintenance, Customer support and training, analytics and reporting.

Duration

Indefinitely, for as long as the Agreement is in force, and until the Customer either a) asks for the personal data to be deleted, or b) asks for the data to be returned, with any copies being deleted by Panaseer.

For processing by (sub-) processors, also specify subject matter, nature and duration of the processing.

Any sub-processors, as Included in the sub-processor List, will be used solely to process the same subject matter and personal data as already processed by Panaseer, and to the same nature and with the same duration as already described in this Annex 1.

ANNEX 2

Technical and Organisational Measures

1. Storage limitation

Panaseer is required to limit the storage of personal data processed for the Customer by:

- Deleting personal data stored concerning users of the service within 12 months after time of collection.
- Upon request from the Customer delete personal data concerning users of services or customer service representatives.

2. Information security policy

Panaseer shall have a documented information security policy, which is defined and approved by the management, published and communicated to its staff and other relevant parties.

3. Information security organisation

Panaseer shall have staff with appointed responsibilities for ensuring an appropriate information security.

4. Staff security

4.1 Panaseer shall in the recruitment process conduct adequate controls for applicants according to applicable legislations and ethic codes, which shall be in proportion to the business operations, the categories of personal data given access to and risk levels.

4.2 Panaseer shall ensure that all personnel with access to personal data processed for the Customer have a confidentiality obligation towards Panaseer and receive continued information security training.

4.3 Panaseer shall have an employee offboarding process which includes removal of access rights and return of IT equipment.

5. Personal data handling

5.1 Panaseer shall handle personal data processed for the Customer as confidential information.

6. Access Control

6.1 Users shall only have access to personal data, personal data processing resources, networks and network services that are needed to perform their duties and for which they have received explicit permission to access.

6.2 Panaseer shall prevent unauthorised access to personal data processed for the Customer by (at least) implementing activity logs which register user activities and can give information about what personal data has been exposed to unauthorised access, modification, erasure or destruction.

7. Physical security

7.1 Physical access to Panaseer's systems and processing environment shall be restricted to authorised personnel.

7.2 Physical access to personal data processed for the Customer shall be restricted and require identifiable and personal authentication scheme.

7.3 Equipment shall be placed and protected to minimise risks for environment related threats and dangers and unauthorised access.

8. Communication security

8.1 Personal data processing resources containing personal data or which are part of the system of the processing shall be protected.

8.2 Panaseer shall apply up-to-date security measures for electronic messages to actively protect against viruses, malware, ransomware and other harmful software.

8.3 Development, test and production environments shall be separated to minimise the risk for unauthorised access or changes in the production and other environments.

8.4 Data from the Customer cannot be used in test or development environments.

9. Confidentiality and non-disclosure agreements

Panaseer shall ensure that requirements for confidentiality or non-disclosure agreements reflecting Panaseer needs for the protection of information are identified, regularly reviewed and documented.

10. Information security awareness, education and training

Panaseer shall ensure all of its employees and, where relevant, contractors, receive appropriate awareness education and training and regular updates in organisational policies and procedures. as relevant for their position. All employees shall be subject to regular phishing tests.

11. Acceptable use of assets

Panaseer shall implement rules for the acceptable use of information and of assets associated with information and information processing facilities are identified, documented and implemented.

12. Information Classification

Panaseer shall ensure that all information assets are classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.

13. Information systems audit controls

Panaseer shall implement carefully planned and agreed upon audit requirements and activities involving verification of operational systems to minimize disruptions to business processes.

14. Networks controls

Panaseer shall ensure networks are managed and controlled to protect information in systems and applications and ensure groups of information services, users and information systems are appropriately segregated.

15. Secure system engineering principles

Panaseer shall ensure principles for engineering secure systems are established, documented, maintained and applied to any information system implementation efforts.

16. System security and acceptance testing

Panaseer shall ensure testing of security functionality is carried out during development and that acceptance testing programs and related criteria are established for new information systems, upgrades and new versions. Panaseer shall ensure test data is selected carefully, protected and controlled.

17. Electronic messaging

Panaseer shall ensure information involved in electronic messaging shall be appropriately protected.

18. Controls against malware

Panaseer shall implement detection prevention and recovery controls to protect against malware, combined with appropriate user awareness.

19. Management of technical vulnerabilities

Panaseer shall implement technical vulnerabilities mitigation to reduce exposure to such vulnerabilities and ensure appropriate measures are taken to address the associated risk.

20. Planning information security continuity

Panaseer shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or a disaster.

21. Information backup

Panaseer shall implement a backup policy defining the requirements for backup of information, software and systems.

22. Access control policy

Panaseer shall have an access control policy which is documented and reviewed periodically based on business and information security requirements.

23. Policy on the use of cryptographic controls

Panaseer shall have developed and implemented a policy on the use of cryptographic controls for the protection of the information.

24. Secure disposal or re-use of equipment

Panaseer shall ensure all equipment items containing storage media are verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

25. Media Disposal

Panaseer shall ensure all media is disposed of securely when no longer required, using formal procedures.

26. Reporting and responding to information security events

Panaseer shall ensure information security events are reported through appropriate management channels as quickly as possible and shall ensure information security incidents are responded to in accordance with the documented procedures.

Appendix A

EU Standard Contractual Clauses for the transfer of personal data to third countries

Where the transfer involves a transfer of EEA Protected Data outside of the EEA ("Ex-EEA Transfer") and the mechanisms referenced in Clause 7.2 (i) or (ii) of this DPA do not apply, such transfer shall be governed by the EU SCCs.

1. Controller-Processor

Considering that the processing activities between the Parties constitute a Controller-Processor relationship, Module 2 of the EU SCCs shall apply and shall be completed as follows:

i. All explanatory notes and footnotes deleted.

ii. As the Ex-EEA Transfer is a controller to processor transfer, only the provisions relating to Module 2 apply to such ex-EEA Transfer, and the provisions relating only to Modules 1, 3 and 4 are deleted and shall not apply to such ex-EEA Transfer.

iii. Clause 7 the Optional provision shall not apply.

iv. In respect of Clause 9 (sub-processors), Option 2 general written authorisation applies, and the minimum time period for the data importer to specifically inform the data exporter in writing of any intended changes to that list in accordance with Clause 9 shall be 7 days.

v. The "OPTION" in Clause 11(a) shall not apply and the wording in square brackets in that Clause shall be deleted.

vi. In respect of Clause 13(a) (supervision), the following wording shall apply: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I C, shall act as competent supervisory authority.

vii. In respect of Clause 17 (governing law), Option 1 shall apply, and the Member State governing law shall be the law of Ireland.

viii. In respect of Clause 18 (choice of forum and jurisdiction), the relevant courts shall be the courts of Ireland.

2. Appendix to the EU SCCs

In all cases, the Appendix to the EU SCCs shall be completed as follows:

- Annex I (A) is completed as follows in accordance with the data flows between the Parties:

  Data Exporter – where Customer is the exporter, this shall be completed with the Customer details as set out in this DPA; where Panaseer is the exporter, this shall be the Panaseer entity as defined in this DPA.

  Data Importer – where Customer is the importer, this shall be completed with the Customer details as set out in this DPA; where Panaseer is the importer, this shall be the Panaseer entity as defined in this DPA.
- Annex I (B) is completed with the information set out in Annex 1 of this DPA.

- Annex I (C) is the supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under the EU SCCs in relation to the offering of goods or services to them.

- Annex II is completed with the information set out at Annex 2 of this DPA.

- Annex III is completed with the information set out in the Sub-processor List.

3. Swiss Addendum to the EU SCCs

The Parties agree that for transfers of personal data from Switzerland subject exclusively to the Data Protection Laws and Regulations of Switzerland ("Swiss Data Protection Laws"), the terms of the EU SCCs shall be amended and supplemented as specified by the relevant guidance of the Swiss Federal Data Protection and Information Commissioner, and the following provisions shall apply:

i. General and specific references in the EU SCCs to EU GDPR, or EU or Member State Law, shall have the same meaning as the equivalent reference in Swiss Data Protection Laws.

ii. In respect of data transfers governed by Swiss Data Protection Laws, the EU SCCs also apply to the transfer of information relating to an identified or identifiable legal entity where such information is protected similarly as personal data under Swiss Data Protection Laws until such laws are amended to no longer apply to a legal entity.

iii. Where the data exporter is established in Switzerland or falls within the territorial scope of application of Swiss Data Protection Laws and Regulations, the Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws and Regulations.

iv. In respect of disputes, the choice of forum and jurisdiction as set out in the EU SCCs shall apply. For data subjects habitually resident in Switzerland, the law and courts of Switzerland are an alternative place of jurisdiction.

Appendix B

UK STANDARD CONTRACTUAL CLAUSES

The Parties agree that to the extent there are transfers of Personal Data from the United Kingdom, and the mechanisms referenced in Clause 7.2 (i) or (ii) of this DPA do not apply, the UK SCCs shall apply and shall be incorporated hereby by reference.

In addition, where the UK SCCs identify optional provisions (or provisions with multiple options) the following shall apply in the following manner:

Part 1 - Tables:

- **Table 1:** For the purposes of Table 1 of the UK SCCs, the names of the parties, their roles and their details shall be set out as per the details stated in this DPA and the Agreement.

- **Table 2:** For the purposes of Table 2 of the UK SCCs, the boxes shall be completed with the information Appendix A which sets out the version of the EU SCCs which this UK SCCs are appended to, including the selected modules, clauses, optional provisions and Appendix Information. For the avoidance of doubt, England and Wales laws shall apply and English courts shall have jurisdiction.

- **Table 3:** "Appendix Information" is completed as set out in Annexes 1, 2 and 3 of this DPA.

- **Table 4:** For the purposes of Table 4, the parties agree that neither the Importer nor the Exporter may end the UK Addendum as set out in Section 19.

Part 2 Mandatory Clauses:

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, are incorporated by reference.

Appendix C

CCPA ADDENDUM

This CCPA Addendum complements the DPA between Panaseer and Customer, and shall apply only to the extent Panaseer processes personal information of Californian residents that Customer provides or makes available to Panaseer in connection with the Agreement.

1. **Definitions**

i. The terms "***consumer***", "***device***", "***personal information***", "***processing***", "***sell***", "***service provider***" and "***third party***" shall have the meaning ascribed to them in the CCPA. For the avoidance of doubt, 'personal information' includes, but is not limited to, the types of data described in Annex A to the DPA. Capitalized terms not defined in this Addendum shall have the meanings set forth in the Agreement.

ii. "***Permitted Service Provider***" means third party service providers engaged by Panaseer to process Customer Personal Information on Panaseer's behalf to assist in the performance of the Services that are set out in clause 8 of the DPA.

iii. "***Personal Information***" means all personal information of California residents that Customer provides or makes available to Panaseer, or that Panaseer otherwise processes on Customer's behalf, in each case, in connection with Panaseer's provision of the Services pursuant to the Agreement.

2. Processing of Personal Information

i. This Addendum applies to the collection, retention, use, disclosure, and sale of Personal Information.

ii. Customer is a business and appoints Panaseer as a service provider to process the Personal Information on behalf of Customer.

iii. Panaseer's collection, retention, use, disclosure, or sale of Personal Information for its own purposes independent of Customer's use of the Services specified in the Agreement are outside the scope of this Addendum.

iv. Panaseer will comply with the CCPA and treat all Personal Data subject to the CCPA in accordance with the provisions of the CCPA. Panaseer will not:

(a) sell Personal Information;
(b) retain, use or disclose any Personal Information for any purpose other than for the specific purpose of providing the Services, including retaining, using or disclosing Personal Information for a commercial purpose other than providing the Services; or
(c) retain, use or disclose Personal Information outside of the direct business relationship between Panaseer and Customer.

v. The parties acknowledge and agree that the Processing of Personal Information authorized by Customer's instructions described in the Agreement and the DPA is integral to and encompassed by Panaseer's provision of the Services and the direct business relationship between the parties. The parties acknowledge and agree that Panaseer access to Customer's Data does not constitute part of the consideration exchanged by the parties in respect of the Agreement.

vi. To the extent that any usage data is considered Personal Information, Panaseer is the business with respect to such data and will Process such data in accordance with its privacy policy found at https://panaseer.com/privacy-policy/

vii. Panaseer and Customer certify that they understand and will comply with the obligations and restrictions set forth in the DPA and the Agreement as required under the CCPA.