Operata

Data Processing Agreement (DPA)

March 2026

Data Protection Provision

The following constitutes the Data Protection Provisions:

1. Processing of personal data

1.1 Definitions

a. In this Data Protection Provision, the following terms shall have the following corresponding definitions. Where not defined below, any capitalised terms shall have the definitions as set out in the Agreement:

i. "Applicable Data Protection Laws" means all laws, statutes, regulations and subordinate legislation relating to the processing, privacy and/or use of Personal Data applicable to the Processor and/or the Services, including:

(A) in the European Union and/or European Economic Area: the General Data Protection Regulation (EU) 2016/679 ("GDPR"), the ePrivacy Directive (2002/58/EC) and all relevant member state implementing laws;

(B) in the United Kingdom: the UK GDPR, the Data Protection Act 2018, and the Privacy and Electronic Communications Regulations 2003;

(C) in Australia: the Privacy Act 1988 (Cth) as amended by the Privacy and Other Legislation Amendment Act 2024, and the Australian Privacy Principles;

(D) in the United States: the California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act of 2020 ("CPRA"), and any other applicable state privacy laws; and

(E) any judicial or administrative interpretation, guidance,

guidelines, codes of practice, approved codes of conduct or approved certification mechanisms issued by any relevant Supervisory Authority.

ii. "Automated Decision-Making" means any processing of Personal Data that involves the use of automated systems, including artificial intelligence or machine learning models, to make decisions or generate outputs that may significantly affect Data Subjects.

iii. "Controller, Data Subject, Personal Data, Processor" and processing shall have the respective meanings given to them in applicable Data Protection Laws from time to time (and related expressions, including process, processing, processed, and processes shall be construed accordingly) and international organization and Personal Data Breach shall have the respective meanings given to them in the GDPR;

iv. "Data Protection Laws" means any Applicable Law relating to the processing, privacy, and/or use of Personal Data, as applicable to the Customer, the Supplier and/or the Services;

v. "Government Authority Request" means any subpoena, warrant or other judicial, regulatory, governmental, or administrative order, proceeding, demand or request (whether formal or informal) by a government or quasi-governmental or other regulatory authority (including law enforcement or intelligence agencies) seeking or requiring access to or disclosure of Protected Data.

vi. "Protected Data" means Personal Data received from or on behalf of the Customer, or otherwise obtained in connection with the performance of Customer's obligations under this Agreement;

vii. "Standard Contractual Clauses" or "SCCs" means the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries, as amended or replaced from time to time, and the UK International Data Transfer Addendum to the EU SCCs as applicable.

viii. "Sub-Processor" means any agent, subcontractor or other third party engaged by Supplier (or by any other Sub-Processor) for carrying out any processing activities in respect of the Protected Data; and

ix. "Supervisory Authority" means any regulator, authority or body

Operata

responsible for administering Data Protection Laws, including the Office of the Australian Information Commissioner (OAIC), the UK Information Commissioner's Office (ICO), and relevant EU data protection authorities.

2. Compliance with Data Protection Laws

a. The Parties agree that:

i. In respect of Customer's Protected Data, Customer is a Controller and that Supplier is a Processor; and

ii. In respect of any Protected Data for which Customer's customer is the data controller, Customer is a Processor and Supplier is a Sub-Processor.

iii. For the purposes of processing Protected Data pursuant to this Agreement, Supplier shall, and shall ensure its Sub-Processors and each of Supplier's Personnel shall, at all times comply with all Data Protection Laws in connection with the processing of Protected Data and the provision of the Services. Nothing in this Agreement relieves the Supplier of any responsibilities or liabilities under Data Protection Laws.

b. Supplier shall indemnify and keep indemnified Customer against all losses, claims, damages, liabilities, fines, penalties, costs, charges, sanctions, expenses, compensation paid to Data Subjects, demands and legal and other professional costs arising out of or in connection with any breach by the Supplier of its obligations under this Agreement.

3. Instructions

a. Supplier shall only process (and shall ensure Supplier Personnel only process) the Protected Data in accordance with the Agreement and Customer's documented instructions, except where otherwise required by applicable law (and in such a case shall inform the Customer of that legal requirement before processing, unless applicable law prevents it doing so on important grounds of public interest). Supplier shall immediately inform Customer if any instruction relating to the Protected Data infringes or may infringe any Data Protection Law.

Operata

4. Security

a. Supplier shall at all times implement and maintain appropriate technical and organisational measures to protect Protected Data against accidental, unauthorised or unlawful destruction, loss, alteration, disclosure or access, including but not limited to:

i. encryption of Personal Data in transit and at rest;

ii. measures to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

iii. measures to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;

iv. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures; and

v. multi-factor authentication and role-based access controls for systems that Process Protected Data.

b. Supplier maintains SOC 2 Type II certification and will maintain such certification (or any equivalent or successor certification) for the duration of the Agreement. Upon Customer's request, Supplier shall promptly provide a copy of its applicable then-current SOC 2 report.

c. Supplier shall promptly notify Customer of any qualified report or material weaknesses identified in any compliance assessment. Within sixty (60) days, Supplier shall resolve such material weaknesses and notify Customer of the resolution.

5. Sub-processing and personnel

a. Supplier shall:

i. notify Customer at least sixty (60) days before engaging any new Sub-Processor to process Protected Data and give Customer an opportunity to object. If Customer reasonably objects, Supplier will not use such Sub-Processor or, if not feasible, will allow Customer to terminate the impacted orders without liability;

ii. maintain a current list of Sub-Processors, which shall be made available to Customer upon request;

iii. ensure that access to Protected Data is limited to the authorised persons who

Operata

need access to it to supply the Services;

iv. prior to the relevant Sub-Processor carrying out any processing activities, appoint each Sub-Processor under a binding written contract containing obligations no less protective than those under this Agreement;

v. remain fully liable to Customer under this Agreement for all the acts and omissions of each Sub-Processor;

vi. ensure that all persons authorised to process Protected Data are reliable, adequately trained on data protection compliance, informed of the confidential nature of the Protected Data, and subject to binding obligations of confidentiality; and

vii. provide relevant details and a copy of each agreement with a Sub-Processor to Customer on request.

---

6. Assistance

a. Supplier shall (at its own cost and expense):

i. promptly provide such information and assistance as Customer may require in relation to the fulfilment of Customer's obligations to respond to Data Subject requests under Chapter III of the GDPR (and any similar obligations under applicable Data Protection Laws); and

ii. provide such information, co-operation and other assistance to Customer as Customer reasonably requires to ensure compliance with Customer's obligations under Data Protection Laws, including with respect to:

(A) security of processing;

(B) data protection impact assessments (as such term is defined in Data Protection Laws);

(C) prior consultation with a Supervisory Authority regarding high risk processing; and

(D) any remedial action and/or notifications to be taken in response to any Personal Data Breach.

b. Supplier shall record and refer all requests and communications received from Data Subjects or any Supervisory Authority to Customer which relate to any Protected Data promptly (and in any event within five (5) business days of receipt) and shall not respond to any without Customer's express written approval unless required by law.

Operata

7. International transfers

a. Supplier shall not process or transfer Protected Data to countries outside the European Economic Area, the United Kingdom, or Australia without Customer's prior written consent.

b. Where Protected Data is transferred to a country that has not been recognised as providing an adequate level of data protection, Supplier shall:

i. enter into the Standard Contractual Clauses (EU 2021/914) and, where applicable, the UK International Data Transfer Addendum;

ii. complete a data transfer impact assessment with Customer; and

iii. implement any supplementary measures necessary to ensure an adequate level of protection.

c. Should any Supervisory Authority or court determine that a data transfer mechanism used herein is no longer valid, the Parties shall promptly implement an approved alternative mechanism.

8. Records and audit

a. Supplier shall maintain complete, accurate and up to date written records of all categories of processing activities carried out on behalf of Customer, including all information necessary to demonstrate compliance with this Agreement and the information referred to in Articles 30(1) and 30(2) of the GDPR. Supplier shall provide copies of such records to Customer within thirty (30) days of request.

b. Supplier shall make available to Customer such information as is reasonably required to demonstrate compliance with their respective obligations under this Agreement and the Data Protection Laws, and allow for, permit and contribute to audits, including inspections, by Customer or an auditor mandated by Customer, upon reasonable prior notice during normal business hours.

9. Breach

a. Supplier shall promptly (and in any event within seventy-two (72) hours) notify Customer if it (or any of its Sub-Processors) suspects or becomes aware of any Personal Data Breach in respect of any Protected Data. Such notification shall include:

Operata

i. a description of the nature of the Personal Data Breach, including where possible the categories and approximate number of Data Subjects and records concerned;

ii. the likely consequences of the Personal Data Breach;

iii. the measures taken or proposed to address the Personal Data Breach and mitigate its adverse effects; and

iv. the name and contact details of Supplier's data protection contact.

b. Supplier shall provide all information as Customer requires to report the breach to a Supervisory Authority and to notify affected Data Subjects under Data Protection Laws.

---

10. AI and Automated Processing

a. Where Supplier uses any form of Automated Decision-Making, including artificial intelligence or machine learning systems, in the Processing of Protected Data, Supplier shall:

i. disclose to Customer the nature, purpose, and logic of such Automated Decision-Making before it is implemented;

ii. conduct and document a data protection impact assessment for any Automated Decision-Making that may significantly affect Data Subjects;

iii. ensure meaningful human oversight where required by Applicable Data Protection Laws;

iv. not use Protected Data for the training, development, or improvement of AI or machine learning models without Customer's prior written consent;

v. comply with the EU Artificial Intelligence Act (Regulation (EU) 2024/1689) to the extent applicable; and

vi. provide Customer with sufficient information to enable compliance with any transparency or disclosure obligations relating to automated processing.

---

11. CCPA/CPRA Compliance

a. To the extent the CPRA applies, Supplier shall not:

i. sell or share Protected Data;

ii. retain, use or disclose Protected Data for any purpose other than the business

purposes specified in the Agreement, or outside of the direct business relationship between Customer and Supplier; or

iii. combine Protected Data with personal information received from or on behalf of another person(s), or collected from Supplier's own interactions with individuals, unless permitted by the CPRA.

b. Supplier certifies that it understands and will comply with the restrictions set forth in this section and Applicable Data Protection Laws.

12. Government Authority Requests

a. Supplier shall have procedures in place to respond to Government Authority Requests and shall promptly notify Customer in writing of any such request, so that Customer may contest, seek to narrow, or seek a protective order or other appropriate remedy.

b. If disclosure is legally compelled, Supplier shall ensure only the minimum required amount of Protected Data is provided and that disclosure is conducted securely.

c. Unless prohibited by law, Supplier shall not voluntarily disclose Protected Data to any government authority without Customer's prior written consent.

13. Deletion/return

a. Supplier shall (and shall ensure that each of the Sub-Processors and Supplier Personnel shall) as soon as reasonably practicable, at Customer's written request, either securely delete or securely return all the Protected Data to Customer after the earlier of:

b. the end of the provision of the relevant Services related to processing of such Protected Data; or

c. once processing by Supplier of any Protected Data is no longer required for the purpose of Supplier's performance of its relevant obligations under this Agreement, and securely delete existing copies (except to the extent that storage of any such data is required by applicable law and, if so, Supplier shall inform Customer of any such requirement).

d. Supplier shall provide written certification to Customer that all Protected Data has been securely deleted or returned within ninety (90) days of the effective date of termination of the Agreement. Deletion shall be performed in accordance with

generally accepted industry standards (e.g., NIST SP 800-88).

e. This clause shall survive termination or expiry of this Agreement for any reason.

14. Cost

a. Each Party shall perform all of its obligations under this Agreement at no additional cost to the other Party, unless otherwise agreed in writing.

Execution

This Data Processing Agreement is incorporated into and forms part of the Agreement. It shall take effect upon the Controller's execution of an Order Form or other agreement that references this Data Processing Agreement.

By signing an Order Form that incorporates this Data Processing Agreement, each Party acknowledges that it has read, understood, and agrees to be bound by the terms set forth herein.