CPA Australia European Data Processing Agreement

Effective 3 May 2018

Background

(A) CPA Australia Group processes personal information concerning data subjects located within the European Economic Area ("**European Personal Data**") in certain circumstances for its business operations. Further information about the types of personal information that CPA Australia Group processes in its business and the categories of data subjects to whom the personal information relates can be found at: https://www.cpaaustralia.com.au/utilities/privacy/privacy-policy (the "**CPA Australia Privacy Policy**").

(B) This document sets out the terms and conditions: (a) on which CPA Australia Group permits suppliers and other parties to process the European Personal Data that CPA Australia Group processes in its business operations; and (b) on which CPA Australia may process European Personal Data received by such suppliers and other third parties concerning data subjects located within the European Economic Area ("**Data Processing Agreement**").

(C) This Data Processing Agreement shall apply to and be incorporated by reference within each contract (each, a "**Supply Agreement**") that the CPA Australia Group has in place with any such third party (each, a "**Supplier**") and will be subject to its terms. It shall take priority over any other agreement or contract that CPA Australia Group may have in place with the Supplier to the extent of any conflict or inconsistency between their provisions relating to the privacy and security of European Personal Data.

(D) Clause 7 sets out definitions for terms used in this Data Processing Agreement and principles as to how it will be interpreted.

Operative Provisions

1. Relationship of the parties

CPA Australia Group and the Supplier may each process various types of European Personal Data in relation to their respective business operations.

Each party shall comply with its obligations under this Data Processing Agreement and under Applicable Privacy Law with respect to the types of European Personal Data that it processes and according to its responsibilities as a controller, processor or joint controller (as appropriate) for the relevant European Personal Data.

2. Controller obligations

Whenever a Party is acting in a capacity as a controller in relation to European Personal Data, it shall comply in all respects with Applicable Privacy Law including:

(a) by processing such data fairly and lawfully; and

by implementing appropriate technical and organisational measures to protect such European Personal Data against Security Incidents.

3. Joint controller obligations

Where each of the parties is acting as a joint controller with each other in relation to European Personal Data, they shall each:

(a) comply with their obligations under clause 2;

(b) provide all assistance reasonably required by the other party in order for that other party to comply with such obligations, including with respect to data subject access requests; and

(c) cooperate to ensure that each data subject is given any notices that are required under Applicable Privacy Law with respect to the processing that the parties undertake.

4. Processor obligations

Where a party (the "**Processor**") is processing Personal Data on behalf of the other party, whether as a processor or sub-processor, and not as a controller or joint controller, the following provisions shall apply:

4.1. *Purpose limitation*

The Processor shall process the European Personal Data as a processor (or sub-processor) as necessary to perform its obligations under this Agreement and strictly in accordance with the documented instructions of the Controller (the "**Permitted Purpose**"), except where otherwise required by any applicable European Union law. In no event shall the Processor process the European Personal Data for its own purposes or those of any third party.

4.2. *Confidentiality of processing*

The Processor shall ensure that any person that it authorises to process the European Personal Data (including the Processor's staff, agents and subcontractors) (an "**Authorised Person**") shall be subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty), and shall not permit any person to process the European Personal Data who is not under such a duty of confidentiality. The Processor shall ensure that all Authorised Persons process the Data only as necessary for the Permitted Purpose.

4.3. *Security*

The processor shall implement appropriate technical and organisational measures to protect the European Personal Data (i) from accidental or unlawful destruction, and (ii) loss, alteration, unauthorised disclosure of, or access to the European Personal Data (a "**Security Incident**"). Such measures shall have regard to 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 for the rights and freedoms of natural persons.

4.4. *Subprocessing*

The Processor shall not subcontract any processing of the European Personal Data to a third party subprocessor without the prior written consent of the other party. The parties may agree a list of approved subprocessors by separate written agreement and, if so, the Processor shall maintain and provide updated copies of this list to the other party when it adds or removes subprocessors in accordance with this clause. If the other party refuses to consent to the Processor's appointment of a third party subprocessor on grounds relating to the protection of the European Personal Data, then either the Processor will not appoint the subprocessor or the other party may elect to suspend or terminate its Supply Agreement without penalty.

4.5. *Cooperation and data subjects' rights*

The Processor shall provide all reasonable and timely assistance (including by appropriate technical and organisational measures) to the Controller (at its own expense) to enable the Controller to respond to: (i) any request from a data subject to exercise any of its rights under Applicable Privacy Law (including its rights of access, correction, objection, erasure and data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the processing of the European Personal Data. In the event that any such request, correspondence, enquiry or

complaint is made directly to the Processor, the Processor shall promptly inform the Controller providing full details of the same.

4.6. *Data Protection Impact Assessment*

If the Processor believes or becomes aware that its processing of the European Personal Data is likely to result in a high risk to the data protection rights and freedoms of data subjects, it shall promptly inform the Controller and provide the Controller with all such reasonable and timely assistance as the Controller may require in order to conduct a data protection impact assessment and, if necessary, consult with its relevant data protection authority.

4.7. *Security incidents*

Upon becoming aware of a Security Incident, the Processor shall inform the Controller without undue delay and shall provide all such timely information and cooperation as the Controller may require in order for the Controller to fulfil its data breach reporting obligations under (and in accordance with the timescales required by) Applicable Privacy Law. The Processor shall further take all such measures and actions as are necessary to remedy or mitigate the effects of the Security Incident and shall keep the Controller informed of all developments in connection with the Security Incident.

4.8. *Deletion or return of European Personal Data*

Upon termination or expiry of this Agreement, the Processor shall (at the Controller's election) destroy or return to the Controller all European Personal Data (including all copies of the European Personal Data) in its possession or control (including any European Personal Data subcontracted to a third party for processing). This requirement shall not apply to the extent that the Processor is required by any EU (or any EU Member State) law to retain some or all of the European Personal Data, in which event the Processor shall isolate and protect the European Personal Data from any further processing except to the extent required by such law.

4.9. *Records*

The Processor shall maintain a record of all categories of processing activities carried out on behalf of the Controller, containing: (i) the name and contact details of the processor or processors and of each controller on behalf of which the Processor is acting and, where applicable, of the controller's or processor's representative, and the data protection officer; (ii) the categories of processing carried out on behalf of each controller; (iii) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation; and (iv) where possible, a general description of the technical and organisational security measures implemented by the Processor in accordance with clause 4.3 (Security) ("**Processing Records**"). The Processor shall make available such Processing Records to the Controller within five (5) working days following receipt of a request for such Processing Records from the Controller.

4.10. *Audit*

The Processor shall permit the Controller (or its appointed third party auditors) to audit the Processor's compliance with this clause, and shall make available to the Controller all information, systems and staff necessary for the Controller (or its third party auditors) to conduct such audit. The Processor acknowledges that the Controller (or its third party auditors) may enter its premises for the purposes of conducting this audit, provided that the Controller gives it reasonable prior notice of its intention to audit, conducts its audit during normal business hours, and takes all reasonable measures to prevent unnecessary disruption to the Processor's operations. The Controller will not exercise its audit rights more than once in any twelve (12) calendar month period, except (i) if and when required by instruction of a competent data protection authority; or (ii) the Controller believes a further audit is necessary due to a Security Incident suffered by the Processor.

5. International transfers

5.1. Where a Data Importer processes European Personal Data as a Controller in a territory outside of the EEA that is not an Adequate Territory, then the C2C Model Clauses will be incorporated into this Agreement by reference and will apply to the processing as follows:

(a) each Data Exporter will be deemed to have entered into the C2C Model Clauses in its own name and on its own behalf in relation to the European Personal Data disclosed to the Data Importer to the extent it processes the European Personal Data as a Controller;

(b) each Data Importer will be deemed to have entered into the C2C Model Clauses in its own name and on its own behalf in relation to the European Personal Data disclosed to it by the Data Exporter(s);

(c) under the definitions section of the C2C Model Clauses option h(i) (the data protection laws of the country in which the data exporter is established) will be deemed to have been selected;

(d) the provisions of the Data Processing Schedule including any of its Annexes or, if the Supply Agreement Parties have not agreed a Data Processing Schedule, the C2C Model Clauses shall be deemed to refer to those aspects of the CPA Australia Privacy Policy which contain the relevant information referred to in Schedule 1;

(e) the optional illustrative commercial clauses will be deemed to have been deleted; and

(f) where and to the extent that the C2C Model Clauses apply pursuant to this clause 5, if there is any conflict between this Agreement and the C2C Model Clauses, the C2C Model Clauses will prevail.

5.2. Where a Data Importer Processes European Personal Data as a Processor that originated in the EEA in a territory outside of the EEA that is not an Adequate Territory then the C2P Model Clauses will be incorporated into this Agreement by reference and will apply to the processing as follows:

(a) each Data Exporter will be deemed to have entered into the C2P Model Clauses in its own name and on its own behalf in relation to the European Personal Data disclosed to the Data Importer to the extent it processes the European Personal Data as a processor;

(b) each Data Importer will be deemed to have entered into the C2P Model Clauses in its own name and on its own behalf in relation to the European Personal Data disclosed to it by the Data Exporter(s);

(c) the provisions of the Data Processing Schedule including any of its Annexes or, if the Supply Agreement Parties have not agreed a Data Processing Schedule, then the C2P Model Clauses shall be deemed to refer to those aspects of the CPA Australia Privacy Policy which contain the relevant information referred to in Schedule 1;

(d) the provisions of any security measures agreed in the Supply Agreement will be deemed to be set out in Appendix 2 to the C2P Model Clauses;

(e) the optional illustrative indemnification clause will be deemed to have been deleted; and

(f) where and to the extent that the C2P Model Clauses apply pursuant to this clause 5, if there is any conflict between this Agreement and the C2P Model Clauses, the C2P Model Clauses will prevail.

5.3. Where a Data Importer processes European Personal Data that originated in a non-EEA territory (the "**Exporting Territory**") in a territory which is different from the Exporting Territory (the "**Importing Territory**"), then, the Data Importer will Process such European Personal Data to a standard consistent with the Applicable Privacy Law(s) of the Exporting Country. In such circumstances, the Data Exporter shall inform the Data Importer about the standards that may be required of it by the Applicable Privacy Law(s) of the Exporting Territory and about its responsibilities under the Applicable Privacy Law(s) of the Exporting Territory (whether acting as a Controller or Processor or under any other legal classification according to such Applicable Privacy Law(s)), and shall cooperate fully with the Data Importer to ensure that its Processing of the European Personal Data is consistent with such standards.

5.4. In any event, if any Applicable Privacy Law(s) conflict with the provisions of this Agreement, then to the extent of such conflict:

(a) where the standard of data protection required by Applicable Privacy Law(s) exceeds the standard required by this Agreement, the Data Importer shall Process the European Personal Data to a standard consistent with Applicable Privacy Law(s); and

(b) where the standard of data protection required by this Agreement exceeds the standard required by Applicable Privacy Law(s), the Data Importer shall Process the European Personal Data to a standard consistent with this Agreement.

6. Costs

Each party shall bear its own costs for complying with its obligations under this Addendum and shall not be entitled to any charge any additional fees to the other party for such compliance, except as may otherwise be expressly agreed in writing by the other party.

7. Definitions

In this Data Processing Agreement, these terms shall have the meanings given to them below:

(a) "**Adequate Territory**" means a territory outside of the European Economic Area that has been designated by the European Commission as ensuring an adequate level of protection pursuant to Applicable Privacy Law;

(b) "**Applicable Privacy Law**" shall mean: (i) prior to 25 May 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data; (ii) on and after 25 May 2018, 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, and repealing Directive 95/46/EC (General Data Protection Regulation); (iii) any applicable national laws and regulations that implement the laws referred to in sub-paragraphs (i) and (ii); and (iv) any other laws and regulations relating to privacy or data protection;

(c) "**C2C Model Clauses**" means model clauses for the transfer of European Personal Data to Controllers established in third countries approved by the European

Commission from time to time, the approved version of which in force as at the Effective Date is that set out in the European Commission's Decision 2004/915/EC of 27 December 2004 (available online at http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm), as such model clauses may be amended or superseded by the European Commission from time to time.

(d) "**C2P Model Clauses**" means model clauses for the transfer of European Personal Data to Processors established in third countries approved by the European Commission from time to time, the approved version of which in force as at the Effective Date is that set out in the European Commission's Decision 2004/915/EC of 27 December 2004 (available online at http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm), as such model clauses may be amended or superseded by the European Commission from time to time.

(e) "**controller**", "**processor**", "**data subject**", "**personal data**" and "**processing**" (and "**process**") shall have the meanings given in Applicable Privacy Law. Where Applicable Privacy Law does not prescribe or refer to a controller, processor or joint controller, each party shall be classified according to whatever classification applies under Applicable Privacy Law and mostly closely aligns with the role of controller, processor or joint controller under Applicable Privacy Law in the European Union.

(f) "**CPA Australia**" shall mean CPA Australia Limited or the relevant affiliate of CPA Australia Limited who is a Supply Agreement Party;

(g) "**CPA Australia Group**" means: (i) CPA Australia Limited; (ii) every company or corporation that directly or indirectly controls, is controlled by, or is under common control with, CPA Australia Limited; and (iii) each overseas or international branch of any entity described in paragraphs (i) or (ii), whether or not such overseas or international branch has separate legal personality from the other entity or not.

(h) "**Data Exporter**" means a Supply Agreement Party that discloses European Personal Data to another Supply Agreement Party in accordance with that Supply Agreement and this Data Processing Agreement.

(i) "**Data Importer**" means a Supply Agreement Party that receives European Personal Data from another Supply Agreement Party in accordance with that Supply Agreement and this Data Processing Agreement. "**Data Processing Schedule**" means, in relation to a Supply Agreement, a version of Schedule 1 (Data Processing Schedule) as agreed between the Supply Agreement Parties.

(j) "**Supply Agreement Party**" means a party to a Supply Agreement (whether CPA Australia or a Supplier).

Schedule 1

Data Processing Schedule

This Schedule, including any annex to it, describes the types of European Personal Data disclosed by Data Exporters, the categories of data subjects to which such European Personal Data relates and the purposes for which that European Personal Data may be processed by the Data Importers.

Data exporter

Data importer

Data subjects

Purpose of processing

Categories of data

Recipients

Sensitive personal data

Other useful information

Data protection registration information of data exporter (where applicable)

Contact points for data protection enquiries