

# ChargeDesk Data Processing Agreement ("DPA")

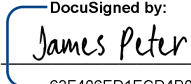
(SEPTEMBER 2021)

## PARTIES

1. Peter Industries Pty Ltd, acting as The Trustee for Peter Family Trust, trading as ChargeDesk Pty Ltd (ABN 13 588 984 088) registered in QLD, Australia ("**ChargeDesk**"); and
2. \_\_\_\_\_  
(the "**Customer**").

## EXECUTION

The parties have indicated their acceptance of this entire Agreement, including any Annexes, by executing it below.

On behalf of the <b>CUSTOMER</b> ;	On behalf of <b>CHARGEDESK</b> ;
Signature: _____	Signature:  _____ <small>63F406ED1ECD4B0...</small>
Date: _____	Date: <u>09/28/2021</u>
Name: _____	Name: <u>James Peter</u>
Title: _____	Title: <u>Co-Founder</u>
Email: _____	Email: <u>james@chargedesk.com</u>
Address: _____	Address: <u>12 Dulku Close</u> <u>Port Douglas, Australia</u>

This signed agreement must be submitted to [privacy@chargedesk.com](mailto:privacy@chargedesk.com). Upon receipt of the validly completed DPA by ChargeDesk at this email address, this DPA will become legally binding.

## BACKGROUND

This Data Processing Agreement ("DPA"), forms part of the ChargeDesk Terms of Service (available at <https://chargedesk.com/terms-of-service>), or other written or electronic agreement, by and between ChargeDesk and the undersigned Customer for certain services (collectively, the "Service").

In connection with the Service, the parties anticipate that ChargeDesk may process outside of the European Economic Area ("EEA"), certain Personal Data in respect of which the Customer may be a data controller under applicable EU Data Protection Laws. The parties have agreed to enter into this DPA in order to ensure that adequate safeguards are put in place with respect to the protection of such Personal Data as required by EU Data Protection Laws.

## **AGREEMENT**

### **1. Definitions**

1.1 In this Agreement, except to the extent expressly provided otherwise:

**"Agreement"** means this agreement including any Annexes, and any amendments to this Agreement from time to time;

**"Customer Personal Data"** means any Personal Data that is processed by ChargeDesk on behalf of the Customer under or in relation to this Agreement;

**"Data Protection Laws"** means all applicable laws relating to the processing of Personal Data including, while it is in force and applicable to Customer Personal Data, the General Data Protection Regulation (Regulation (EU) 2016/679);

**"Effective Date"** means the date upon which the Customer first uses the Service;

**"Main Agreement"** means the ChargeDesk Terms of Service (available at <https://chargedesk.com/terms-of-service>) or other written or electronic agreement, by and between ChargeDesk and the undersigned Customer;

**"Personal Data"** has the meaning given to it in the Data Protection Laws;

**"Service"** means any functionality located on ChargeDesk.com, or through any Application published by ChargeDesk, or through any ChargeDesk APIs, or through any software or other websites that interface with ChargeDesk.com its Applications or APIs;

**"Annex"** means any annex attached to the main body of this Agreement; and

**"Term"** means the term of this Agreement, commencing in accordance with Clause 3.1 and ending in accordance with Clause 3.2.

### **2. Supplemental**

2.1 This Agreement supplements the Main Agreement.

2.2 Any capitalised terms that are:

- (a) used in this Agreement;
- (b) defined in the Main Agreement; and

(c) not defined in this Agreement,

shall in this Agreement have the meanings given to them in the Main Agreement.

- 2.3 If there is a conflict between this Agreement and the Main Agreement, then this Agreement shall take precedence.
- 2.4 This Agreement shall automatically terminate upon the termination of the Main Agreement.
- 2.5 The Main Agreement shall automatically terminate upon the termination of this Agreement.

### **3. Term**

- 3.1 This Agreement shall come into force upon the Effective Date.
- 3.2 This Agreement shall continue in force indefinitely, subject to termination in accordance with Clause 2.4, 2.5 or 6 or any other provision of this Agreement.

### **4. Data protection**

- 4.1 Each party shall comply with the Data Protection Laws with respect to the processing of the Customer Personal Data.
- 4.2 The Customer warrants to ChargeDesk that it has the legal right to disclose all Personal Data that it does in fact disclose to ChargeDesk under or in connection with this Agreement.
- 4.3 The Customer shall only supply to ChargeDesk, and ChargeDesk shall only process, in each case under or in relation to this Agreement, the Personal Data of data subjects falling within the categories and types specified in ANNEX I, B. DESCRIPTION OF TRANSFER; and ChargeDesk shall only process the Customer Personal Data for the purposes specified in ANNEX I, B. DESCRIPTION OF TRANSFER.
- 4.4 ChargeDesk shall only process the Customer Personal Data during the Term and for not more than 90 days following the end of the Term, subject to the other provisions of this Clause 4.
- 4.5 ChargeDesk shall only process the Customer Personal Data, as set out in this Agreement or any other document agreed by the parties in writing.
- 4.6 ChargeDesk shall promptly inform the Customer if, in the opinion of ChargeDesk, an instruction of the Customer relating to the processing of the Customer Personal Data infringes the Data Protection Laws.
- 4.7 To the extent any processing of Personal Data by ChargeDesk takes place in any country outside the European Economic Area (except if in an Adequate

Country), the parties agree that the Standard Contractual Clauses approved by the EU authorities under EU Data Protection Laws and included in this Agreement will apply in respect of that processing, and ChargeDesk will comply with the obligations of the 'data importer' in the Standard Contractual Clauses and the Customer will comply with the obligations of the 'data exporter'.

- 4.8 Notwithstanding any other provision of this Agreement, ChargeDesk may process the Customer Personal Data if and to the extent that ChargeDesk is required to do so by applicable law. In such a case, ChargeDesk shall inform the Customer of the legal requirement before processing, unless that law prohibits such information.
- 4.9 ChargeDesk shall take reasonable steps to ensure that only authorized personnel have access to such Personal Data and that any persons whom it authorizes to have access to the Personal Data are under obligations of confidentiality.
- 4.10 ChargeDesk and the Customer shall each implement appropriate technical and organisational measures to ensure an appropriate level of security for the Customer Personal Data, including those measures specified in ANNEX II.
- 4.11 The Customer grants a general authorization to the Processor to appoint third party data center operators, and outsourced marketing, business, engineering and customer support providers as sub-processors to support the performance of the Service.
- 4.12 ChargeDesk includes a list of sub-processors in ANNEX III and will notify you via the Customer Email address specified in this agreement at least thirty (30) days in advance of any changes to this list. If the Customer has a reasonable objection to any new or replacement sub-processor, it shall notify ChargeDesk of such objections in writing within ten (10) days of the notification and the parties will seek to resolve the matter in good faith. If ChargeDesk is reasonably able to provide the Service to the Customer in accordance with the Main Agreement without using the sub-processor and decides in its discretion to do so, then the Customer will have no further rights under this clause 4.12 in respect of the proposed use of the sub-processor. If ChargeDesk requires use of the sub-processor in its discretion and is unable to satisfy the Customer as to the suitability of the sub-processor or the documentation and protections in place between ChargeDesk and the sub-processor, the Customer may terminate the Main Agreement with at least twenty (20) days written notice, solely with respect to the service(s) to which the proposed new sub-processor's processing of Personal Data relates. If the Customer does not provide a timely objection to any new or replacement sub-processor in accordance with this clause 4.12, the Customer will be deemed to have consented to the sub-processor and waived its right to object. ChargeDesk may use a new or replacement sub-processor whilst the objection procedure in this clause 4.12 is in process.
- 4.13 ChargeDesk shall, insofar as possible and taking into account the nature of the processing, take appropriate technical and organisational measures to assist the Customer with the fulfilment of the Customer's obligation to

respond to requests exercising a data subject's rights under the Data Protection Laws.

- 4.14 ChargeDesk shall assist the Customer in ensuring compliance with the obligations relating to the security of processing of personal data, the notification of personal data breaches to the supervisory authority, the communication of personal data breaches to the data subject, data protection impact assessments and prior consultation in relation to high-risk processing under the Data Protection Laws. ChargeDesk shall report any Personal Data breach relating to the Customer Personal Data to the Customer within 72 hours following ChargeDesk becoming aware of the breach. ChargeDesk may charge the Customer at its standard time-based charging rates for any work performed by ChargeDesk at the request of the Customer pursuant to this Clause 4.14.
- 4.15 ChargeDesk shall, in accordance with EU Data Protection Laws, make available to the Customer such information in ChargeDesk's possession or control as the Customer may reasonably request with a view to demonstrating ChargeDesk's compliance with the obligations of data processors under EU Data Protection Law in relation to its processing of Personal Data.
- 4.16 ChargeDesk shall, delete all of the Customer Personal Data after the provision of services relating to the processing according to Clause 5.6 of the Terms of Service, and shall delete existing copies save to the extent that applicable law requires storage of the relevant Personal Data.
- 4.17 ChargeDesk shall allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer in respect of the compliance of ChargeDesk's processing of Customer Personal Data with the Data Protection Laws and this Clause 4. ChargeDesk may charge the Customer at its standard time-based charging rates for any work performed by ChargeDesk at the request of the Customer pursuant to this Clause 4.17.
- 4.18 If any changes or prospective changes to the Data Protection Laws result or will result in one or both parties not complying with the Data Protection Laws in relation to processing of Personal Data carried out under this Agreement, then the parties shall use their best endeavours promptly to agree such variations to this Agreement as may be necessary to remedy such non-compliance.

## **5. Limits upon exclusions of liability**

- 5.1 Nothing in this Agreement will:
  - (a) limit or exclude any liability for death or personal injury resulting from negligence;
  - (b) limit or exclude any liability for fraud or fraudulent misrepresentation;

- (c) limit any liabilities in any way that is not permitted under applicable law; or
- (d) exclude any liabilities that may not be excluded under applicable law.

## **6. Termination**

- 6.1 Either party may terminate this Agreement immediately by giving written notice of termination to the other party if the other party commits a material breach of this Agreement.
- 6.2 Either party may terminate this Agreement immediately by giving written notice of termination to the other party if:
  - (a) the other party:
    - (i) is dissolved;
    - (ii) ceases to conduct all (or substantially all) of its business;
    - (iii) is or becomes unable to pay its debts as they fall due;
    - (iv) is or becomes insolvent or is declared insolvent; or
    - (v) convenes a meeting or makes or proposes to make any arrangement or composition with its creditors;
  - (b) an administrator, administrative receiver, liquidator, receiver, trustee, manager or similar is appointed over any of the assets of the other party;
  - (c) an order is made for the winding up of the other party, or the other party passes a resolution for its winding up (other than for the purpose of a solvent company reorganisation where the resulting entity will assume all the obligations of the other party under this Agreement); or
  - (d) if that other party is an individual:
    - (i) that other party dies;
    - (ii) as a result of illness or incapacity, that other party becomes incapable of managing his or her own affairs; or
    - (iii) that other party is the subject of a bankruptcy petition or order.
- 6.3 ChargeDesk may terminate this Agreement and the Standard Contractual Clauses if ChargeDesk offers alternative mechanisms to Customer that comply with the obligations of the European Union privacy laws for the transfer of Personal Data outside the EEA.

## **7. Effects of termination**

- 7.1 Except to the extent that this Agreement expressly provides otherwise, the termination of this Agreement shall not affect the accrued rights of either party.
- 7.2 ChargeDesk will automatically delete the Customer Personal Data 90 days after this Agreement is terminated. The Customer may request this occurs within 2 business days according to Clause 5.6 of the Terms of Service.

## **8. General**

- 8.1 No breach of any provision of this Agreement shall be waived except with the express written consent of the party not in breach.
- 8.2 If any provision of this Agreement is determined by any court or other competent authority to be unlawful and/or unenforceable, the other provisions of this Agreement will continue in effect. If any unlawful and/or unenforceable provision would be lawful or enforceable if part of it were deleted, that part will be deemed to be deleted, and the rest of the provision will continue in effect (unless that would contradict the clear intention of the parties, in which case the entirety of the relevant provision will be deemed to be deleted).
- 8.3 Neither party may without the prior written consent of the other party assign, transfer, charge, license or otherwise deal in or dispose of any contractual rights or obligations under this Agreement.
- 8.4 This Agreement is made for the benefit of the parties, and is not intended to benefit any third party or be enforceable by any third party. The rights of the parties to terminate, rescind, or agree to any amendment, waiver, variation or settlement under or relating to this Agreement are not subject to the consent of any third party.
- 8.5 Subject to Clause 5, this Agreement shall constitute the entire agreement between the parties in relation to the subject matter of this Agreement, and shall supersede all previous agreements, arrangements and understandings between the parties in respect of that subject matter.

## **9. Interpretation**

- 9.1 In this Agreement, a reference to a statute or statutory provision includes a reference to:
  - (a) that statute or statutory provision as modified, consolidated and/or re-enacted from time to time; and
  - (b) any subordinate legislation made under that statute or statutory provision.
- 9.2 The Clause headings do not affect the interpretation of this Agreement.

- 9.3 References in this Agreement to "calendar months" are to the 12 named periods (January, February and so on) into which a year is divided.
- 9.4 In this Agreement, general words shall not be given a restrictive interpretation by reason of being preceded or followed by words indicating a particular class of acts, matters or things.



## **STANDARD CONTRACTUAL CLAUSES**

MODULE TWO: Transfer Controller to Processor

MODULE THREE: Transfer Processor 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) for the transfer of personal data to a third country.
- (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 - Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);
  - (iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
  - (iv) Clause 12 - Modules Two and Three: Clause 12(a), (d) and (f);
  - (v) Clause 13;
  - (vi) Clause 15.1(c), (d) and (e);
  - (vii) Clause 16(e);
  - (viii) Clause 18 - Modules One, Two and Three: 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*

#### ***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.

### **MODULE TWO: Transfer controller to processor**

#### **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 (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 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.

### **MODULE THREE: Transfer processor to processor**

#### **8.1 Instructions**

- (a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.
- (b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.
- (c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.
- (d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

#### **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 controller, as communicated to the data importer by the data exporter, or 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 personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand 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.

#### **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 rectify or erase 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 controller 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, they 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 subject. 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 or the controller. 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 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, without undue delay, the data exporter and, where appropriate and feasible, the controller 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 data breach, including 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 its controller so that the latter may in turn 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 set out 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 controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (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 of Regulation (EU) 2016/679;
- (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 or the controller 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 controller.
- (c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.
- (d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.
- (e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.
- (f) 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.
- (g) 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*****MODULE TWO: Transfer controller to processor**

- (a) 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 thirty (30) 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. 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, 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.

### **MODULE THREE: Transfer processor to processor**

- (a) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the controller 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 controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).
- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), 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. 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 or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, 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**

## **MODULE TWO: Transfer controller to processor**

- (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.

## **MODULE THREE: Transfer processor to processor**

- (a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.
- (b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. 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 controller, as communicated by 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.

## **MODULE TWO: Transfer controller to processor**

## **MODULE THREE: Transfer processor to processor**

- (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***

#### **MODULE TWO: Transfer controller to processor**

#### **MODULE THREE: Transfer processor to processor**

- (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***

**MODULE TWO: Transfer controller to processor**

**MODULE THREE: Transfer processor to processor**

- (a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, 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***

**MODULE TWO: Transfer controller to processor**

**MODULE THREE: Transfer processor to processor**

- (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;

- (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures 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). For Module Three: The data exporter shall forward the notification to the controller.
- (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 (for Module Three: , if appropriate in consultation with the controller). 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 (for Module Three: the controller or) 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***

#### **MODULE TWO: Transfer controller to processor**

#### **MODULE THREE: Transfer processor to processor**

##### **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.

For Module Three: The data exporter shall forward the notification to the controller.

- (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.). For Module Three: The data exporter shall forward the information to the controller.
- (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. For Module Three: The data exporter shall make the assessment available to the controller.
- (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 (for Module Three: and the controller) 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***

#### **MODULE TWO: Transfer controller to processor**



### **MODULE THREE: Transfer processor to processor**

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 the Republic of Ireland.

#### *Clause 18*

#### ***Choice of forum and jurisdiction***

### **MODULE TWO: Transfer controller to processor**

### **MODULE THREE: Transfer processor to processor**

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (f) The Parties agree that those shall be the courts of the Republic of Ireland.
- (g) 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.
- (h) The Parties agree to submit themselves to the jurisdiction of such courts.

## **ANNEX I**

### **A. LIST OF PARTIES**

**MODULE TWO: Transfer controller to processor**

**MODULE THREE: Transfer processor to processor**

#### **Data exporter:**

Name: Customer as executed in this agreement

Address: Customer Address as executed in this agreement

Contact person's name, position and contact details: Customer name, title, email and address as executed in this agreement

Signature and date: as executed in this agreement

Role (controller/processor): controller/processor

#### **Data importer:**

Name: Peter Industries Pty Ltd, acting as The Trustee for Peter Family Trust, trading as ChargeDesk Pty Ltd (ABN 13 588 984 088)

Address: 12 Dulku Close, Craiglie 4877 QLD, Australia

Contact person's name, position and contact details: James Peter, Co-Founder, [privacy@chargedesk.com](mailto:privacy@chargedesk.com)

Signature and date: as executed in this agreement

Role (controller/processor): processor

### **B. DESCRIPTION OF TRANSFER**

**MODULE TWO: Transfer controller to processor**

**MODULE THREE: Transfer processor to processor**

#### **Categories of Data Subjects**

The data exporter may submit Personal Data to ChargeDesk, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, to the following categories of data subjects:

Prospective and current customers, employees, contact persons of the data exporter's prospective customers or any natural persons authorized by the data exporter to use the services provided by ChargeDesk to the data exporter.

#### **Categories of Personal Data**

The data exporter may submit Personal Data to ChargeDesk, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to, the following categories of Personal Data:

- Name
- Email Address
- Phone Number
- Country
- Billing Address
- Shipping Address
- Username
- IP Address
- Last 4 Digits of Credit Card
- Metadata defined by Controller
- Transaction History with Controller

### **Sensitive Data**

The personal data transferred to ChargeDesk is determined and controlled by the Customer. As such, the Customer controls the content of the personal data transferred to ChargeDesk and is solely responsible for ensuring the legality of the categories of data it may choose to transfer to ChargeDesk. The DPA includes an express prohibition on the transfer of special categories of personal data to ChargeDesk.

The data exporter may not submit special categories of personal data, unless such data complies with Article 9 of the GDPR. In other words, the following types of personal data generally may not be processed:

- Race and ethnicity
- Political, religious, or philosophical beliefs, including union membership
- Health, sex life, and sexual orientation
- Genetic and biometric data (for the purpose of uniquely identification)

### **Frequency of the Transfer**

Continuous

### **Nature of the Processing**

ChargeDesk will perform the following basic processing activities: processing to provide the Service in accordance with the Agreement; processing to perform any steps necessary for the performance of the Agreement; and processing to comply with other reasonable instructions provided by Customer that are consistent with the terms of the Agreement.

### **Purpose of the data transfer and further processing**

To provide the Service in accordance with the Agreement.

### **Period for which the personal data will be retained**

Throughout the Term of the Agreement plus the period from expiry of the Term until deletion of Personal Data by ChargeDesk in accordance with the Agreement.

**C. COMPETENT SUPERVISORY AUTHORITY**

**MODULE TWO: Transfer controller to processor**

**MODULE THREE: Transfer processor to processor**

The member state of the Customer.

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

### **MODULE TWO: Transfer controller to processor**

### **MODULE THREE: Transfer processor to processor**

#### **Measures of encryption of personal data**

- ChargeDesk only processes and stores personal data necessary to provide the Service.
- All data is encrypted in transit and at rest using state-of-the-art encryption protocols.
- ChargeDesk uses a minimum 256-bit key length for asymmetric encryption (2048-bit for RSA).
- Encryption keys are securely stored with limited organisational access.

#### **Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services**

- ChargeDesk tests code for vulnerabilities.
- ChargeDesk employs code reviews for sensitive updates to increase the security of our code.
- Intrusion detection and prevention (IDS/IPS) is deployed in both production and staging environments.
- Production systems run on high-availability systems across multiple availability zones.
- Production data never leaves the production environment and is never used in testing or staging environments.
- We use a Reputation Management System which monitors access points to customer data and automatically blocks any threats it identifies. We use a 'block first, ask questions later' approach and all subsequent requests by a potential threat will also be blocked - only a manual review will lift a block.

#### **Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident**

- ChargeDesk performs at least daily backups of production data.
- Automatic failover capability is deployed for production systems so that individual server failure does not disrupt the service.
- Business continuity plans contain all the information needed to get our business running again after an incident or crisis.

#### **Measures for user identification and authorisation**

- All admin users are provided a unique login and ID.

- All admin functionality requires 2 factor authentication with frequent re-authentication when performing high security functions.
- Admin access is frequently reviewed and the principle of least-privilege is employed.

### **Measures for the protection of data during transmission**

- All data is encrypted in transit using state-of-the-art encryption protocols.
- We do not provide any non-SSL endpoints and only support TLS 1.2 or above
- We use the most modern ciphers and important recent innovations such as Forward Secrecy and Strict Transport Security.
- Encryption is enabled on all internal network transmissions
- ChargeDesk uses a third party enterprise-class web application firewall to restrict access to our services.
- We use a Reputation Management System which monitors access points to customer data and automatically blocks any threats it identifies. We use a 'block first, ask questions later' approach and all subsequent requests by a potential threat will also be blocked - only a manual review will lift a block.

### **Measures for the protection of data during storage**

- All data is encrypted at rest using state-of-the-art encryption protocols.
- ChargeDesk uses a minimum 256-bit key length for asymmetric encryption (2048-bit for RSA).
- Encryption keys are securely stored with limited organisational access.

### **Measures for ensuring physical security of locations at which personal data are processed**

- ChargeDesk leverages Amazon Web Services data center for cloud infrastructure.
- Access to all data centers is strictly controlled.
- All data centers are equipped with 24x7x365 surveillance and biometric access control systems.
- Amazon Web Services data centers are SOC Type II and ISO 27001 certified.
- ChargeDesk employees do not have physical access to Amazon Web Service data centers, servers, network equipment, or storage.

### **Measures for ensuring events logging**

- All access to the production and staging system is logged.
- Access logs are centrally stored and indexed.
- Admin access logs are tied to unique admin IDs.

### **Measures for ensuring system configuration**

- Production systems are deployed and managed with code.
- Management code is reviewed to ensure systems are secure and no insecure defaults are enabled.
- All changes to production environments are logged.

### **Measures for security management & assurance**

- The ChargeDesk Security Policy documents internal security policies
- Assigned employees responsible for Security Policy compliance
- Security training is required for all new employees and renewed at least annually
- All policy documents reviewed at least annually

### **Penetration Testing**

- ChargeDesk undergoes annual penetration testing conducted by an independent third-party.
- For testing, ChargeDesk provides the third-party with access to an isolated clone of chargedesk.com.
- No customer data is exposed to the third-party through penetration testing.

### **Measures for ensuring data minimisation & limited data retention**

- The Main Agreement limits data storage to up to 90 days following account deactivation
- Only the limited data required to provide the Service is imported by default from connected providers.
- Defaults reviewed and set to collect the least amount of data necessary to provide the Service

### **Measures for allowing data portability and ensuring erasure**

- ChargeDesk provides companies with the ability to export data for individual users. This export can also be exposed through self-support pages so individual users can export their own data.
- ChargeDesk provides the ability for companies to delete an entire customer record from a single location.

### **Additional Safeguards - Measures and assurances regarding U.S. government surveillance**

- ChargeDesk uses encryption both in transit and at rest.
- As of the date of this DPA, ChargeDesk has not received any national security orders of the type described in Paragraphs 150-202 of the judgment in the EU Court of Justice Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems.
- ChargeDesk is not eligible to be required to provide information, facilities, or assistance under FISA Section 702; or that no court has found ChargeDesk

to be the type of entity eligible to receive process issued under FISA Section 702: (i) an "electronic communication service provider" within the meaning of 50 U.S.C § 1881(b)(4) or (ii) a member of any of the categories of entities described within that definition.

- ChargeDesk is not the type of provider that is eligible to be subject to upstream collection ("bulk" collection) pursuant to FISA Section 702, as described in paragraphs 62 & 179 of the judgment in the EU Court of Justice Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems ("Schrems II"), and that therefore the only FISA Section 702 process it could be eligible to receive, if it is an "electronic communication service provider" within the meaning of 50 U.S.C § 1881(b)(4), would be based on a specific "targeted selector" i.e., an identifier that is unique to the targeted endpoint of communications subject to the surveillance.
- ChargeDesk shall not comply with any request under FISA for bulk surveillance, i.e., a surveillance demand whereby a targeted account identifier is not identified via a specific "targeted selector" (an identifier that is unique to the targeted endpoint of communications subject to the surveillance).
- ChargeDesk shall use all available legal mechanisms to challenge any demands for data access through the national security process that ChargeDesk receives, as well as any non-disclosure provisions attached thereto.
- ChargeDesk shall take no action pursuant to U.S. Executive Order 12333.
- ChargeDesk will notify the Customer if ChargeDesk can no longer comply with the Standard Contractual Clauses or these Additional Safeguards, without being required to identify the specific provision with which it can no longer comply.



### **ANNEX III – LIST OF SUB-PROCESSORS**

#### **MODULE TWO: Transfer controller to processor**

#### **MODULE THREE: Transfer processor to processor**

The controller has authorised the use of the following sub-processors:

1. Name: Amazon Web Services, Inc

Address: 410 Terry Avenue North, Seattle, WA 98109 USA

Contact details: <https://aws.amazon.com/contact-us/compliance-support/>

Description of processing: Cloud infrastructure services

Website: <https://aws.amazon.com/>

2. Name: Cloudflare, Inc

Address: 01 Townsend Street, San Francisco, California 94107 USA

Contact details: +1 (888) 993-527

Description of processing: Data transmission and security

Website: <https://www.cloudflare.com/>

3. Name: Mailgun Technologies, Inc

Address: 112 E Pecan St. #1135, San Antonio, TX 78205 USA

Contact details: <https://www.mailgun.com/contact/>

Description of processing: Email delivery

Website: <https://www.mailgun.com/>

4. Name: Twilio, Inc

Address: 375 Beale Street Suite 300 San Francisco, CA 94105 USA

Contact details: [privacy@twilio.com](mailto:privacy@twilio.com)

Description of processing: Text message delivery

Website: <https://www.twilio.com/>