DATA PROCESSING AGREEMENT

v202108a

This Data Processing Agreement (**DPA**) is entered between between [Customer who signs-up for Cascade Enterprise product or Customer who executed an Order Form] (**you** or **your**) and Responsis Pty Ltd ABN 26 160 406 100 (**we**, **us** or **our**), together the **Parties** and each a **Party**. This DPA is incorporated into, and is subject to the terms and conditions of, the Terms of Service (**Terms**) entered into between the Parties.

1. Application

1.1 This DPA applies only to the extent that we process personal data which is subject to Regulation (EU) 2016/67 (**Regulation**) on your behalf.

1.2 This DPA is based on Module Two (transfer controller to processor) of the Standard Contractual Clauses implemented under the Commission Implementing Decision (EU) 2021/914 and as set out below under the subheading 'Standard Contractual Clauses – Controller to Processor' (the **Clauses**). The Clauses are considered to provide appropriate safeguards for international data transfers by a controller of personal data processed subject to the Regulation (data exporter) to a processor whose processing of the data is not subject to the Regulation (data importer). The Parties agree that the Clauses will apply for the purpose of such transfers, to the extent we are not subject to the Regulation.

1.3 As per the Commission Implementing Decision (EU) 2021/914, the Parties agree that Module Two of the Clauses (as included below) also sets out the rights and obligations under Article 28(3) and (4) of the Regulation, with respect to the transfer of personal data from a controller to a processor. Accordingly, the Parties agree that the Clauses will apply as an integral part of this DPA to the processing of personal data whether or not:

(a) we are subject to the Regulation; and

(b) there is an international data transfer.

1.4 With regard to the processing of personal data, the Parties acknowledge that:

(a) Annex I.B to the Clauses describes the subject matter and details of the processing of personal data;

(b) you are the controller and data exporter; and

(c) we are the processor and data importer.

1.5 For the avoidance of doubt, this DPA will not apply in instances where we are the controller.

1.6 Where this DPA uses terms which are defined in the Regulation or the Terms, those terms will have the same meaning as in the Regulation or Terms (as relevant).

2. Additional commercial clauses

The additional commercial clauses set out here will apply to the Clauses below. These additional commercial clauses have been drafted on the basis of the express statement in clause 2 of the Clauses which states that the Clauses may be included in a wider contract and that the parties are free to add other clauses provided they do not contradict, directly or indirectly, the Clauses or prejudice the fundamental rights and freedoms of data subjects.

1.7 You represent and warrant to us that Annex I.B has been accurately completed.

1.8 In relation to clause 8.1 of the Clauses, you acknowledge and expressly agree that:

(a) the following is deemed to be your instruction regarding the processing of personal data by us. You instruct us to process the personal data:

(1) to provide the Service, and any related support;

(2) as specified by you during your use of the Service and any related support;

(3) aggregate and anonymize data to create analytics for our use in improving the Service and creating new products and services;

(4) as documented in the Terms;

(5) as documented in this DPA;

(6) in addition to any further documented instructions provided by you; and

(b) an email is sufficient to meet the 'documented' requirement for instructions.

1.9 In relation to clause 8.3 of the Clauses, the Parties agree that where a copy of the Clauses is to be provided to a data subject, only the Clauses forming part of this DPA and not the whole DPA will be provided to the data subject.

1.10 In relation to clause 8.5 of the Clauses, you must notify us of your preference for deletion or return of personal data within 30 days after the end of our provision of the processing services. If you do not notify us of your preference within this timeframe, you will be deemed to have requested deletion of the personal data and we will be entitled to delete such data without any liability to you.

1.11 For the purpose of security of processing under clause 8.6 of the Clauses, you acknowledge and expressly agree that:

(a) the regular checks of security measures referred to under clause 8.6(a) of the Clauses will be carried out annually;

(b) we may update our security measures, including the measures described in Annex II, at any time, provided that such updates and modifications do not result in the degradation of the overall security of our Service;

(c) except as expressly provided by the DPA and the Terms, you are responsible for your secure use of our Service, including:

(1) assessing and using the Service so as to ensure an acceptable level of risk to the personal data you ask us to process;

(2) keeping your and your authorized users' account credentials confidential and secure;

(3) protecting the personal data that you elect to store or transfer outside of the Service (and for which we will have no obligation); and

(d) our notification of, or response to, a personal data breach in accordance with clauses 8.6(c) and (d) of the Clauses, will not be construed as an acknowledgement by us of any fault or liability with respect to the personal data breach.

1.12 In relation to any audits requested under clause 8.9 of the Clauses:

(a) you agree that prior to conducting such an audit, you will request information from us (such as evidence of our relevant certifications) which you require for us to demonstrate our compliance with our obligations under Article 28 of the Regulation and these Clauses. Subject to our confidentiality obligations, we will promptly provide such information;

(b) if the information provided is not sufficient, you may conduct an audit and the Parties agree that the audit will be conducted in accordance with the following specifications:

(1) the audit will be subject to our obligations of confidentiality;

(2) you will not request an audit more than once annually unless there is evidence of non-compliance by us;

(3) you will request an audit by providing us reasonable written notice and 30 days is considered reasonable notice;

(4) if you choose to use an independent auditor, you will be responsible for ensuring the auditor signs an appropriate confidentiality agreement, in a form approved by us, and for paying their fees;

(5) for on-site audits, reasonable professional fees will be agreed with you to compensate us for any time required by our personnel for the purpose of the audit;

(6) prior to any on-site audit, you will work with us to agree the scope, time, duration and fees for that audit;

(7) you will only request access to information for the purpose of good faith fulfillment of your obligations under the Regulation;

(8) you will take all reasonable measures to limit any adverse impact on us; and

(9) if you discover any non-compliance during an audit, you will promptly notify us of the non-compliance and provide us with any information relevant to the non-compliance.

1.13 In relation to clause 9 of the Clauses:

(a) the agreed list of sub-processors is attached as Appendix II to this DPA;

(b) any objection to a sub-processor must be in writing and on reasonable grounds;

(c) in response to any objection to a sub-processor by you, we will do one of the following, at our election:

(1) not appoint the proposed sub-processor;

(2) not disclose any personal data we process on your behalf to the proposed sub-processor;

(3) not disclose any personal data we process on your behalf to the proposed sub-processor until reasonable steps have been taken to address your objections, you have been informed of those reasonable steps and agreed to that sub-processor based on those reasonable steps; or

(4) inform you that you may terminate the Terms immediately by providing written notice to us; and

(d) you agree that the remedies described above in (1) through to (4) above are the only remedies available if you object to any proposed sub-processor.

1.14 In relation to clause 10 of the Clauses:

(a) in notifying you of a data subject request under clause 10(a) and/or providing assistance under clause 10(b), you agree that we may do so via the provision of self-service features via your Account, which you may be able to use, at no additional

cost, to access, port, rectify, delete, object or restrict the use of personal data in connection with your obligations under the Regulation. If self-service is not available or is not sufficient, and it is appropriate to do so, we will provide further assistance in cooperation with you;

(b) you instruct us that we may respond to a request from a data subject to acknowledge the request; and

(c) for the avoidance of doubt, this DPA does not apply where we are a controller and nothing in this DPA will restrict or prohibit us from responding to a request from a data subject where we act as the controller.

1.15 Any assistance we provide to you which either:

(a) extends beyond our obligations under the Regulation or this DPA; or

(b) is required due to your (or your personnel's) act or omission (e.g. a personal data breach caused by your Personnel failing to keep logins confidential) will be at your expense (on a time and materials basis).

1.16 In relation to any requirement for certification to be provided by us under the Clauses, including under clauses 8.5 and 16(d), the Parties agree that we may provide such certification via email.

1.17 In relation to clause 14 of the Clauses:

(a) you acknowledge that there are certain laws in Australia which require that we handle personal data in a manner that varies from some of our obligations under the Clauses;

(b) you acknowledge and expressly agree that with respect to those laws and practices listed below, we have notified you of such laws and practices:

(1) noting the obligation in clause 10 of the Clauses in particular, under the Australian *Privacy Act 1988* (Cth) we are obliged to respond to an access or correction request within a reasonable period of receiving the request and we are obliged to provide access to or correct personal information unless an exception applies. Where we act as a processor for you, we will notify you of a data subject request and, to the extent possible to do so and still meet our obligations under the Privacy Act, we will follow your instructions. We will notify you if we believe we must action a request under the Privacy Act despite your instructions;

(2) noting the obligations in clauses 8.5 and 16(d) of the Clauses in particular, we have data retention obligations in respect of, (i) information which may be relevant in the event of future litigation (e.g. a copy of the contract); (ii) under the Australian *Corporations Act 2001* (Cth), financial records (for at least 7 years) and company records and registers of members, charges and option holders (for at least 5 years); (iii) under the Australian *Income Tax Assessment Act 1936* (Cth), documents relating to our income and expenditure (for at least 5 years); (iv) anything we know may be required in evidence in a judicial proceeding under the relevant crimes acts in Australia, including without limitation, the *Crimes Act 1914* (Cth); and

(3) noting the obligations in clauses 8.5, 14(a), 14(b)(ii) and 16(d) of the Clauses in particular, we may have data retention and disclosure obligations, or obligations to authorize access by authorities to personal data, under Australian national security laws, including the *Australian Security Intelligence Organisation Act 1979* (Cth). We will follow the process in clause 15 of the Clauses if we receive such a disclosure request from a public authority; and

(c) the Parties agree that because Australia is a democratic state, with a legal system underpinned by the rule of law, with laws publicly made, with community participation in the lawmaking process, with public adjudication of laws by courts which are independent from the executive arm of government and laws to combat government corruption or misuse of data, it is the understanding of the Parties that such laws and practices, especially when considered in the context of the safeguards in the Clauses, 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 the Regulation and are not in contradiction with these Clauses. Accordingly, the Parties have no reason to believe that the laws and practices in Australia prevent us from fulfilling our obligations under the Clauses.

1.18 In addition to your termination rights in Clause 16 of the Clauses we will have similar termination rights. Accordingly, you agree that:

(a) you must promptly inform us if you are unable to comply with any part of this DPA, for whatever reason;

(b) in the event that you are in breach of this DPA or unable to comply with this DPA, you will suspend the transfer of personal data to us until compliance is again ensured or this DPA is terminated; and

(c) we may terminate this DPA if:

(1) you do not restore compliance within a reasonable time and in any event within one month of suspension;

(2) you are in substantial or persistent breach of this DPA; or

(3) you fail to comply with a binding decision of a competent court or supervisory authority regarding your obligations under this DPA.

1.19 Subject to the requirements for the allocation of liability in clause 12 of the Clauses, each Party's liability to the other Party, taken together in the aggregate, arising out of or related to this DPA (including the Clauses) will be subject to the exclusions and limitations of liability in the Terms.

1.20 Subject to clause 5 of the Clauses, nothing in this DPA reduces the Parties' obligations under the Terms and all clauses in the Terms will continue to apply in full force and effect.

3. General

1.21 **Counterparts:** This DPA may be executed in any number of counterparts that together will form one instrument.

1.22 **Online execution:** This DPA may be executed by means of such third-party online document execution service as we nominate subject to such execution being in accordance with the applicable terms and conditions of that document execution service.

1.23 **Amendment:** Other than as expressly permitted under this DPA, this DPA may only be amended by written instrument executed by the Parties.

1.24 **Assignment:** A Party must not assign or deal with the whole or any part of its rights or obligations under this DPA without the prior written consent of the other Party (such consent not to be unreasonably withheld).

1.25 **Severance:** If a provision of this DPA is held to be void, invalid, illegal or unenforceable, that provision is to be read down as narrowly as necessary to allow it to be valid or enforceable, failing which, that provision (or that part of that provision) will be severed from this DPA without affecting the validity or enforceability of the remainder of that provision or the other provisions in this DPA.

1.26 **Governing law and disputes:** This DPA will be governed by the laws specified in clause 17 of the Clauses and disputes will be resolved as specified in clause 18 of the Clauses.

STANDARD CONTRACTUAL CLAUSES – CONTROLLER TO PROCESSOR

Section I

1. Purpose and scope

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

(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.

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, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except 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.

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 –Clause 8.1(b), 8.9(a), (c), (d) and (e);
(iii) Clause 9 –Clause 9(a), (c), (d) and (e);
(iv) Clause 12 –Clause 12(a), (d) and (f);
(v) Clause 13;

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(vi) Clause 15.1(c), (d) and (e);
(vii) Clause 16(e);
(viii) Clause 18 –Clause 18(a) and (b);

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

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.

5. Hierarchy

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

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.

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

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 organizational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

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

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

8.2 Purpose limitation

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

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the/its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized 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 pseudonymization, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymization, 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 organizational 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 authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

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

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

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

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

(i) the onward transfer is to a country benefiting 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 defense 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.

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

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.

9. Use of sub-processors

Transfer controller to processor

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

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

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

(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 fulfill 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.

10. Data subject rights

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

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 authorized to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

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

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

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

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

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organization 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.

12. Liability

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

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

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

(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.

13. Supervision

(a) Where the data exporter is established in an EU Member State: 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. Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority. Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located, 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 Obligation in case of access by Public Authorities

14. Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorizing 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 authorizing access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];

(iii) any relevant contractual, technical or organizational 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

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

measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

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

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

15.1 Notification

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

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

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

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

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

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

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

15.2 Review of legality and data minimization

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

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

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

Section IV – Final Provisions

16. Non-compliance with the Clauses and termination

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

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

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

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
(ii) the data importer is in substantial or persistent breach of these Clauses; or
(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

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

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data

importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

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

17. Governing Law

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

18. Choice of forum and jurisdiction

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

(b) The Parties agree that those shall be the courts of Poland, EU.

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

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

APPENDIX I

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

[Customer who signs-up for Cascade Enterprise product or Customer who executed an Order Form]

Data importer(s):

Responsis Pty Ltd of Suite 4.02, 59 Goulburn Street, Haymarket, NSW 2000, Australia

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- Users of the Service
- Any about whom personal data is input into the Service

Categories of personal data transferred

- When a data subject registers for or otherwise uses our subscription service and/or associated mobile application, we may process:
    - name;
    - contact information, such as email address, phone number, billing address and/or mailing address;
    - details of the organization the data subject works for;
    - the data subject's role within that organization;
    - payment details (via our third party PCI-compliant payment processor(s)), for the purpose of payment for our subscription service;
    - any uploads or posts a data subject makes to the Service; and/or
    - any support requests, feedback or other information submitted to us by a data subject; and
    - information we automatically collect from a data subject's use of the Service, including:
        - a data subject's browser session and high level geo-location data (i.e. the country the IP address is linked to), device and network information,

statistics on page views and sessions, acquisition sources, search queries and/or browsing behavior;

- information about a data subject's access and use of the Service, including through the use of Internet cookies, communications with the Service, the type of browser a data subject is using, the type of operating system a data subject is using and the domain name of a data subject's Internet service provider; and
- any additional personal information that a data subject provides to us indirectly, through use of the Service, associated applications, associated social media platforms and/or accounts from which the data subject permits us to collect information.

- Personal data which is input into the Service about a data subject.
- Personal data exported from other business applications into the Service.
- Any other personal data provided to us about a data subject of yours.

Sensitive data transferred *(if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.*

We do not process special categories of data.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

The frequency of transfer is on a continuous basis and based on your use of the Services.

Nature of the processing

The nature of processing is as specified in the Terms, this DPA and as further instructed by you.

Purpose(s) of the data transfer and further processing

The purpose of processing is as specified in the Terms, this DPA and as further instructed by you.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

We will only retain personal data for as long as necessary to fulfil the purposes we are instructed to use it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

To determine the appropriate retention period for personal data, we consider your instructions for its processing and deletion, our obligations to delete it after processing services are complete, the

amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure of the personal data and the applicable legal requirements.

In some circumstances we may anonymize your personal data (so that it can no longer be associated with you) for analytics, research or statistical purposes in which case we may use this anonymize information indefinitely without further notice to you or the relevant data subject.

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

The subject matter, nature and duration of the processing aligns with the subject matter, nature and duration of our processing as set out above and as further described in Appendix 2.

C. COMPETENT SUPERVISORY AUTHORITY

The supervisory authority is: Data Protection Commissioner 21 Fitzwilliam Square D02 RD28 Dublin 2 Tel: +353 76 110 4800 info@dataprotection.ie

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Organizational Security Awareness

- We issue guidance and provide training to business and technical staff on an ongoing basis to ensure systems, data, premises, etc. remain secure. There is a designated information security team responsible for the implementation and continuous improvement of information security.
- Vendors are selected and reviewed to ensure an appropriate information and security posture.

Benefits of AWS Security

- The Cascade system is wholly hosted in the AWS environment, taking full advantage of their industry-leading and continually evolving security processes and practices, compliance and certifications, physical and environmental security, security tools and utilities, etc.

Access Control and Privacy/Confidentiality

- Client Cascade data are treated as confidential.
- Client Cascade data are never shared with third parties without the client's consent.
- Access to the data and the Cascade infrastructure is strictly limited to Cascade staff on a role requirement basis to enable the service to be provided to the client, and is reviewed regularly.
- Access to systems and infrastructure that serve or store client Cascade data is limited by a range of control measures including MFA, IP range restriction, and machine/user-specific keys.

Security Embedded in the SDLC

- Security is built into every stage of the Cascade development lifecycle, and the change control process for the software and infrastructure.
- This includes security testing of the infrastructure and the Cascade application, including internal automated vulnerability scanning, and third-party penetration testing.

Robust Encryption

- Client Cascade Data are encrypted in transit and at rest. Web traffic is encrypted using SSL with TLS1.2 (and non-web traffic with IPSec/SSH tunneling), with data encrypted at rest using AES-256.

Infrastructure Protection

- Infrastructure security tools are deployed to provide WAF, anti-virus, anti-malware, IDS/IPS, and other controls within the Cascade infrastructure.
- The infrastructure is regularly patched using automatic scanning and update mechanisms, as well as administrator monitoring and patching.

Backup and Recovery

- The Cascade system uses the AWS "Availability Zone" architecture, with multiple, redundant, geographically separated data centers, and an automatic fail-over capability. Cascade clients can have very high confidence in Cascade's availability.
- Client Cascade data are backed up regularly using the AWS backup facilities, providing the capability to recover from large scale infrastructure failure.

Logging and Monitoring

- AWS native utilities, plus additional tools, are used to provide logging and monitoring of traffic, activity, configuration changes, performance etc. in the Cascade infrastructure, with logs being stored in a robust and tamper-protected format in the AWS environment.
- Logs are monitored by automated mechanisms with processes to alert administrators to non-standard behaviors.

Incident Response

- We have incident response processes covering data loss, technology attacks, etc.

cascade

APPENDIX II

AGREED LIST OF SUB-PROCESSORS

You, as the controller, have authorized the use of the following sub-processors:

Sub-Processor	Purpose	Primary / Other Locations	Link
Amazon Web Services, Inc.	Hosting of the Cascade system and supporting processes	USA / EU, Australia, Canada	aws.amazon.com
Chargebee, Inc	Subscription processing	USA	www.chargebee.com
Google, Inc.	Emailing and file handling infrastructure	USA / Australia	www.google.com
Hubspot, Inc.	Central contact and marketing database	USA	www.hubspot.com
Intercom, Inc.	Helpdesk platform	USA	www.intercom.com
Hull, Inc.	Customer data aggregation and processing	USA	www.hull.io
Planhat, Inc	Customer success management database	Sweden	www.planhat.com
Segment.io, Inc.	Customer data routing between systems	USA	www.segment.com