Customer Data Processing Agreement

This Customer Data Processing Agreement reflects the requirements of the European Data Protection Regulation (“GDPR”) as it comes into effect on May 25, 2018. Bench´s products and services offered in the European Union are GDPR ready and this DPA provides you with the necessary documentation of this readiness.

This Data Processing Agreement (“DPA”) is an addendum to the Master Services Agreement (“Agreement”) between Bench Media Pty Ltd or Bench APAC Pte Ltd as applicable (“Bench”) and the Customer (within the meaning of the Agreement). All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement. Customer enters into this DPA on behalf of itself and, to the extent required under Data Protection Laws, in the name and on behalf of its Authorized Affiliates (defined below).

This revised DPA applies to any Insertion Orders or Agreements entered into after 27 September 2021, and any Insertion Orders or Agreements entered into prior to that date are still subject to the prior DPA accessible at the following link: https://drive.google.com/file/d/1MGsH22mlFvI_yCxWWUXLXyB30Xhh7_vy/view?usp=sharing

The parties agree as follows:

1. Definitions

“Affiliate” means an entity that directly or indirectly Controls, is Controlled by or is under common Control with an entity.

“Authorized Affiliate” means any of Customer Affiliate(s) permitted to or otherwise receiving the benefit of the Services pursuant to the Agreement.

“Control” means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The term “Controlled” shall be construed accordingly.

“Controller” means an entity that determines the purposes and means of the processing of Personal Data.

“Customer Data” means any data that Bench and/or its Affiliates processes on behalf of Customer in the course of providing the Services under the Agreement.

“Data Protection Laws” means all data protection and privacy laws and regulations applicable to the processing of Personal Data under the Agreement, including, where applicable, EU Data Protection Law.

“EU Data Protection Law” means (i) prior to May 25, 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of Personal Data and on the free movement of such data (“Directive”) and on and after May 25, 2018, Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation) (“GDPR”); and (ii) Directive 2002/58/EC concerning the processing of Personal Data and the protection of privacy in the electronic communications sector and applicable national implementations of it (in each case, as may be amended, superseded or replaced).

“Personal Data” means any Customer Data relating to an identified or identifiable natural person to the extent that such information is protected as personal data under applicable Data Protection Law.

“Processor” means an entity that processes Personal Data on behalf of the Controller.

“Processing” has the meaning given to it in the GDPR and “process”, “processes” and “processed” shall be interpreted accordingly.

“SCCs” means the standard contractual clauses for processors as approved by the European Commission or Swiss Federal Data Protection Authority (as applicable) which are incorporated into this DPA.

“Security Incident” means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data.

“Services” means any product or service provided by Bench to Customer pursuant to and as more particularly described in the Agreement.

“Sub-processor” means any Processor engaged by Bench or its Affiliates to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA. Sub-processors may include third parties or any Bench Affiliate.

2. Scope and Applicability of this DPA

2.1 This DPA applies where and only to the extent that Bench processes Personal Data on behalf of the Customer in the course of providing the Services and such Personal Data is subject to Data Protection Laws of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom. The parties agree to comply with the terms and conditions in this DPA in connection with such Personal Data.

2.2 Role of the Parties. As between Bench and Customer, Customer is the Controller of Personal Data and Bench shall process Personal Data only as a Processor on behalf of Customer. Nothing in the Agreement or this DPA shall prevent Bench from using or sharing any data that Bench would otherwise collect and process independently of Customer's use of the Services.

2.3 Customer Obligations. Customer agrees that (i) it shall comply with its obligations as a Controller under Data Protection Laws in respect of its processing of Personal Data and any processing instructions it issues to Bench; and (ii) it has provided notice and obtained (or shall obtain) all consents and rights necessary under Data Protection Laws for Bench to process Personal Data and provide the Services pursuant to the Agreement and this DPA.

2.4 Bench Processing of Personal Data. As a Processor, Bench shall process Personal Data only for the following purposes: (i) processing to perform the Services in accordance with the Agreement; (ii) processing to perform any steps necessary for the performance of the Agreement; and (iii) to comply with other reasonable instructions provided by Customer to the extent they are consistent with the terms of this Agreement and only in accordance with Customer’s documented lawful instructions. The parties agree that this DPA and the Agreement set out the Customer’s complete and final instructions to Bench in relation to the processing of Personal Data and processing outside the scope of these instructions (if any) shall require prior written agreement between Customer and Bench.

2.5 Nature of the Data. Bench handles Customer Data provided by Customer. Such Customer Data may contain special categories of data depending on how the Services are used by Customer. The Customer Data may be subject to the following process activities: (i) storage and other processing necessary to provide, maintain and improve the Services provided to Customer; (ii) to provide customer and technical support to Customer; and (iii) disclosures as required by law or otherwise set forth in the Agreement.

2.6 Bench Data. Notwithstanding anything to the contrary in the Agreement (including this DPA), Customer acknowledges that Bench shall have a right to use and disclose data relating to and/or obtained in connection with the operation, support and/or use of

the Services for its legitimate business purposes, such as billing, account management, technical support, product development and sales and marketing. To the extent any such data is considered personal data under Data Protection Laws, Bench is the Controller of such data and accordingly shall process such data in compliance with Data Protection Laws.

3. Subprocessing

3.1 Authorized Sub-processors. Customer agrees that Bench may engage Sub-processors to process Personal Data on Customer's behalf. The Sub-processors currently engaged by Bench and authorized by Customer are listed in Annex A and can be requested by Customer.

3.3 Sub-processor Obligations. Bench shall: (i) enter into a written agreement with the Sub-processor imposing data protection terms that require the Sub-processor to protect the Personal Data to the standard required by Data Protection Laws; and (ii) remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause Bench to breach any of its obligations under this DPA.

3.4 Changes to Sub-processors. Bench shall update the list of Authorized Sub-processors from time to time and the Customer shall have deemed to accept any changes by accepting the Master Services Agreement with Bench.

3.5 Objection to Sub-processors. Customer may object in writing to Bench’s appointment of a new Sub-processor on reasonable grounds relating to data protection by notifying Bench promptly in writing within five (5) calendar days of receipt of Bench’s notice in accordance with Section 3.3. Such notice shall explain the reasonable grounds for the objection. In such event, the parties shall discuss such concerns in good faith with a view to achieving commercially reasonable resolution. If this is not possible, either party may terminate the applicable Services that cannot be provided by Bench without the use of the objected-to-new Sub-processor.

4. Security

4.1 Security Measures. Bench shall implement and maintain appropriate technical and organizational security measures to protect Personal Data from Security Incidents and to preserve the security and confidentiality of the Personal Data, in accordance with Bench's security standards described in Exhibit A, Annex II (“Security Measures”).

4.2 Confidentiality of Processing. Bench shall ensure that any person who is authorized by Bench to process Personal Data (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

4.3 Security Incident Response. Upon becoming aware of a Security Incident, Bench shall notify Customer without undue delay and shall provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer.

4.4 Updates to Security Measures. Customer acknowledges that the Security Measures are subject to technical progress and development and that Bench may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by the Customer.

5. Security Reports and Audits

5.1 Bench shall maintain records of its security standards. Upon Customer's written request, Bench shall provide (on a confidential basis) copies of relevant certifications, audit report summaries and/or other documentation reasonably required by Customer to verify Bench's compliance with this DPA. Bench shall further provide written responses (on a confidential basis) to all reasonable requests for information made by Customer, including responses to information security and audit questionnaires, that Customer (acting reasonably) considers necessary to confirm Bench's compliance with this DPA, provided that Customer shall not exercise this right more than once per year.

6. International Transfers

6.1 Processing Locations. Bench stores and processes EU Data (defined below) in data centers located inside and outside the European Union. All other Customer Data may be transferred and processed in the United States and anywhere in the world where Customer, its Affiliates and/or its Sub-processors maintain data processing operations. Bench shall implement appropriate safeguards to protect the Personal Data, wherever it is processed, in accordance with the requirements of Data Protection Laws.

6.2 Transfer Mechanism: Notwithstanding Section 6.1, to the extent Bench processes or transfers (directly or via onward transfer) Personal Data under this DPA from the European Union, the European Economic Area and/or their member states and Switzerland (“EU Data”) in or to countries which do not ensure an adequate level of data

protection within the meaning of applicable Data Protection Laws of the foregoing territories, the parties agree to abide by and process EU Data in compliance with the SCCs in the form set out in Exhibit A. For the purposes of the descriptions in the SCCs, Bench agrees that it is the "data importer" and Customer is the "data exporter" (notwithstanding that Customer may itself be an entity located outside Europe). Customer hereby authorises any transfer of EU Data to, or access to EU Data from, such destinations outside the EU subject to any of these measures having been taken.

7. Return or Deletion of Data

7.1 Upon deactivation of the Services, all Personal Data shall be deleted within 90 days subject to full customer payment of any outstanding invoices, save that this requirement shall not apply to the extent Bench is required by applicable law to retain some or all of the Personal Data, or to Personal Data it has archived on back-up systems, which such Personal Data Bench shall securely isolate and protect from any further processing, except to the extent required by applicable law.

8. Cooperation

8.1 To the extent that Customer is unable to independently access the relevant Personal Data within the Services, Bench shall (at Customer's expense) take into account the nature of the processing, provide reasonable cooperation to assist Customer by appropriate technical and organizational measures, in so far as is possible, to respond to any requests from individuals or applicable data protection authorities relating to the processing of Personal Data under the Agreement. In the event that any such request is made directly to Bench, Bench shall not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. If Bench is required to respond to such a request, Bench shall promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

8.2 To the extent Bench is required under Data Protection Law, Bench shall (at Customer's expense) provide reasonably requested information regarding Bench's processing of Personal Data under the Agreement to enable the Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by law.

9. Miscellaneous

9.1 Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict.

9.2 This DPA is a part of and incorporated into the Agreement so references to "Agreement" in the Agreement shall include this DPA.

9.3 In no event shall any party limit its liability with respect to any individual's data protection rights under this DPA or otherwise.

9.4 This DPA shall be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by Data Protection Laws.

Exhibit B – Standard Contractual Clauses

STANDARD CONTRACTUAL CLAUSES

The standard contractual clauses set out in the Exhibit are considered to provide appropriate safeguards within the meaning of Article 46(1) and (2)(c) of Regulation (EU) 2016/679 for the transfer by a controller or processor of personal data processed subject to that Regulation (data exporter) to a controller or (sub-)processor whose processing of the data is not subject to that Regulation (data importer).

The standard contractual clauses also set out the rights and obligations of controllers and processors with respect to the matters referred to in Article 28(3) and (4) of Regulation (EU) 2016/679, as regards the transfer of personal data from a controller to a processor, or from a processor to a sub-processor.

Execution of the Agreement by the Customer includes execution of these standard contractual clauses.

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 One: Clause 8.5 (e) and Clause 8.9(b); 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); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); 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); Module Four: Clause 18.

(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.

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.

Clause 9

Use of sub-processors

(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 1 week 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.

Clause 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 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.

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.

(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

(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

(a)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 behaviour 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 OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 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 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).

(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. 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.

Clause 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 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.

(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 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

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 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 Ireland.

(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

ANNEX I

A. LIST OF PARTIES

Data exporter(s): The data exporter is the Customer.

Name: As per Agreement

Address: As per Agreement

Contact person's name, position and contact details: As per Agreement

Activities relevant to the data transferred under these Clauses: use of the Services of the Data Importer

Signature and date: As per Agreement

Role (controller/processor): Controller

Data importer(s):

Name: Bench Media Pty Ltd, a company incorporated in Australia.

Address: Level 10, 201 Pacific Highway, St Leonards NSW 2065

Contact person's name, position and contact details: Shai Luft, Chief Operations Officer, shai.luft@benchmedia.com

Signature and date: as per the Agreement

Role (controller/processor): Processor

OR

Name: Bench APAC Pte Ltd, a company incorporated in Singapore.

Address: 160 Robinson Road #14-04, Singapore Business Federation Center, Singapore (068914)

Contact person's name, position and contact details: Shai Luft, Chief Operations Officer, shai.luft@benchmedia.com

Signature and date: as per the Agreement

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

The personal data transferred concern the following categories of data subjects:

The personal data transferred by the data exporter is determined and controlled by the data exporter, in its sole discretion, and may include (without limitation) the personal data of:

- Employees, contractors and temporary workers (current, former, prospective) of data exporter;
- Data exporter's collaborators/contact persons (natural persons) or employees, contractors or temporary workers of legal entity collaborators/contact persons (current, prospective, former);
- Customers, clients, visitors, users and other data subjects of data exporter's goods, services and applications;
- Partners, stakeholders or individuals who actively collaborate, communicate or otherwise interact with employees of the data exporter and/or use communication tools such as apps and websites provided by the data exporter;
- Stakeholders or individuals who passively interact with data exporter (e.g., because they are the subject of an investigation, research or mentioned in documents or correspondence from or to the data exporter).

Categories of personal data transferred

The personal data transferred concern the following categories of data:

The personal data that may be transferred by the data exporter is determined and controlled by the data exporter, in its sole discretion, and may include (without limitation) the following categories of personal data:

Any data (including personal data) inputted into the Services by a Customer, which may include basic personal information, contact details, identity documents, employment details, images and video, authentication data, commercial information, location data, device identification, internet activity and so on.

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

Continuous basis for the duration of the Agreement.

Nature of the processing

The personal data transferred is processed by the data importer to provide the Services pursuant to the Agreement and the DPA, and in accordance with the processing activities described in the Agreement and the DPA.

Purpose(s) of the data transfer and further processing

To facilitate the provision of the Services.

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

For the entire duration in which the data exporter receives Services from the data importer or during which the Agreement remain on foot, or as otherwise stated in this DPA or the Agreement.

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

Same subject matter, nature and duration as above.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Irish Data Protection Commission

ANNEX II

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

In this Annex II, capitalised terms have the same meaning as in the main body of the DPA.

Measures of pseudonymisation and encryption of personal data

Where Customer Data is provided in hashed format, Bench will keep such Customer Data hashed.

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

Bench's Customer, employment, and contractor agreements contain strict confidentiality obligations.

Measures for ensuring the ability to restore availability and access to Personal Data in a timely manner in the event of a physical or technical incident.

Bench performs regular backups of Customer Data.

Processes for regular testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of processing.

Bench maintains a risk-based assessment security program. The framework for Bench's security program includes administrative, organizational, technical, and physical safeguards reasonably designed to protect the Services and confidentiality, integrity, and availability of Customer Data.

Measures for user identification and authorization.

Bench personnel are required to use unique user access credentials and passwords for authorization. Bench personnel are authorized to access Customer Data based on their job function, role and responsibilities, and such access requires approval prior to access provisioning. Access is promptly removed upon role change or termination.

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

Bench headquarters and office spaces have a physical security program that manages visitors, building entrances, and overall office security.

Measures for ensuring limited data retention.

Customers unilaterally determine what Customer Data they route through the Bench Services and how the Services are configured. As such, Bench operates on a shared responsibility model. If a Customer is unable to delete Customer Data via the self-services functionality of the Services, then Bench deletes Customer Data upon the Customer's written request, within the timeframe specified in the DPA and in accordance with Data Protection Laws.

Measures for allowing data portability and ensuring erasure.

If a Customer is unable to use self-service functionality, Bench specifies in the DPA that it will provide assistance to such Customer as may reasonably be require to comply with Customer's obligations under Data Protection Laws to respond to requests from individuals to exercise their rights under Data Protection Laws (e.g., rights of data access, rectification, erasure, restriction, portability and objection). If Bench receives a request from a data subject in relation to their Customer Data, Bench will advise the data subject

to submit their request to Customer, and Customer will be responsible for responding to any such request.

For transfers to sub-processors, also describe the specific technical and organisational measures to be taken by the [sub]- processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the Bench.

When Bench engages a sub-processor under this DPA, Bench and the sub-processor enter into an agreement with data protection terms substantially similar to those contained herein. Each sub-processor agreement must ensure that Bench is able to meet its obligations to Customer. In addition to implementing technical and organisational measures to protect personal data, sub-processors must a) notify Bench in the event of a Security Incident so Bench may notify Customer; b) delete data when instructed by Bench in accordance with Customer's instructions to Bench; c) not engage additional sub-processors without authorization; d) not change the location where data is processed; or e) process data in a manner which conflicts with Customer's instructions to Bench.

ANNEX III

LIST OF SUB-PROCESSORS

The data exporter has authorised the use of the sub-processors as per this sheet.