

## DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") is entered into as of the date of last signature below ("Effective Date") between Watermelon Express, Inc. dba BenchPrep ("BenchPrep"), a Delaware corporation with its principal place of business at 111 S. Wacker Drive, Suite 1200, Chicago, IL 60606, and Company Name ("Customer"), a Place and Type of Incorporation with its principal place of business at Address, and forms part of the Master SaaS Agreement ("Agreement") between BenchPrep and Customer. The terms used in this DPA shall have the meanings set forth in this DPA. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect.

For and in consideration of the representations and promises of the parties set forth herein, and other good and valuable consideration the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

### 1. DEFINITIONS.

In addition to the capitalized terms in Schedule A, all capitalized terms shall have the meaning ascribed to them herein this Schedule, and for the purposes of this Schedule, shall govern and control in the event of any conflict, including the following:

**1.1** In this DPA, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

**1.1.1 Adequacy Decision** means, for a jurisdiction with Privacy Laws that have data transfer restrictions, a country that the Supervisory Authority or other body in such jurisdiction recognizes as providing an adequate level of data protection as required by such jurisdiction's Privacy Laws such that transfer to that country shall be permitted without additional requirements;

**1.1.2 Affiliate** means any entity which now or in the future controls, is controlled by, or is under common control with the signatory to this DPA, with "control" defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of such person or entity, whether through the ownership of voting securities, by contract, or otherwise;

**1.1.3 Data Controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data, and in the context of this DPA shall mean the Customer;

**1.1.4 Data Processing Instructions** means the Processing instructions set out in Annex 1 of this Schedule E;

**1.1.5 Data Processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Data Controller, and in the context of this DPA shall mean BenchPrep;

**1.1.6 Information Security Schedule** means the information security, technical and organizational measures specified in the Information Security Schedule attached as Schedule D to this Agreement, as may be updated from time to time;

**1.1.7 Personal Data** shall have the meaning set out in, and will be interpreted in accordance with Privacy Laws, and in the context of this DPA, shall mean the personal data in Customer Data, Processed by BenchPrep in accordance with the Services as outlined in the Data Processing Instructions, which relates to a Data Subject;

**1.1.8 Personal Data Breach** means Unauthorized Access leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed;

**1.1.9 Process or Processing** means any operation or set of operations that is performed upon Personal Data in connection with the Services, whether or not by automatic means, such as access, collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, return or destruction, as described in the Data Processing Instructions;

**1.1.10 Restricted Transfer** means:

**1.1.10.1** a transfer of Personal Data from Customer to BenchPrep; or

**1.1.10.2** an onward transfer of Personal Data from BenchPrep to a Subprocessor,

in each case, where such transfer outside of jurisdiction of Customer would be prohibited by Privacy Laws in the absence of an approved method of transfer, including through (a) an Adequacy Decision, (b) Standard Contractual Clauses, or (c) by the terms of other recognised forms of data transfer agreements or processes;

**1.1.11 Services** means the services and other activities to be supplied to or carried out by or on behalf of BenchPrep for Customer pursuant to the Agreement;

**1.1.12 Standard Contractual Clauses** means the contractual clauses approved by a Supervisory Authority pursuant to Privacy Laws, as may be updated from time to time, which provides for multi-jurisdictional transfer of Personal Data from one jurisdiction to another where such transfer would otherwise be a Restricted Transfer;

**1.1.13 Subprocessor** means any third party (including any third party and any BenchPrep Affiliate) appointed by or on behalf of BenchPrep to undertake Processing in connection with the Services, which are listed in Annex 1 of this Schedule E; and

**1.1.14 Supervisory Authority** means an independent public authority which is established in a jurisdiction under Privacy Laws with competence in matters pertaining to data protection.

**1.2** The word "include" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

**1.3** The terms used in this DPA shall have the meanings set forth in this DPA provided that capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement. Except as modified below, the terms of the Agreement shall remain unchanged and in full force and effect.

### 2. PROCESSING OF PERSONAL DATA

**2.1** BenchPrep will not:

**2.1.1** Process Personal Data other than on Customer's documented instructions (set out in this DPA and in the Agreement) unless Processing is required by a Supervisory Authority; or

**2.1.2** sell Personal Data received from Customer or obtained in connection with the provision of the Services to Customer.

#### **2.2 Customer on behalf of itself and each Customer Affiliate:**

**2.2.1** instructs BenchPrep:

**2.2.1.1** to Process Personal Data; and

**2.2.1.2** in particular, transfer Personal Data to any country or territory;

in each case as reasonably necessary for the provision of the Services and consistent with this DPA.

**2.3** The Data Processing Instructions sets out the subject matter and other details regarding the Processing of the Personal Data contemplated as part of

the Services, including Data Subjects, categories of Personal Data, special categories of Personal Data, Subprocessors and description of Processing.

### **3. BENCHPREP PERSONNEL**

BenchPrep shall ensure that persons authorized to undertake Processing of the Personal Data have:

**3.1** committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality in respect of the Personal Data; and

**3.2** undertaken appropriate training in relation to protection of Personal Data.

### **4. SECURITY**

**4.1** Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, BenchPrep shall in relation to the Personal Data implement appropriate technical and organizational measures designed to provide a level of security appropriate to that risk in the provision of the Services and for the purposes of this DPA BenchPrep's technical and organizational measures are set out in the Information Security Schedule.

**4.2** In assessing the appropriate level of security, BenchPrep shall take account in particular of the risks that are presented by Processing.

### **5. SUBPROCESSING.**

**5.1** BenchPrep shall only appoint Subprocessors which enable BenchPrep to comply with Privacy Laws. Customer authorises BenchPrep to appoint Subprocessors in accordance with this Section 5 subject to any restrictions or conditions expressly set out in the Agreement. Subprocessors appointed as at the effective date of this DPA are listed in the Data Processing Instructions. BenchPrep shall remain liable to Customer for the performance of that Subprocessor's obligations subject to the Agreement.

**5.2** Notwithstanding any notice requirements in the Agreement, before BenchPrep engages any new Subprocessor, BenchPrep shall give Customer notice of such appointment, including details of the Processing to be undertaken by the proposed Subprocessor. In addition to any other notifications, BenchPrep may provide such notice by updating the list of Subprocessors in the Data Processing Instructions. Customer may notify BenchPrep of any objections (on reasonable grounds related to Privacy Laws) to the proposed Subprocessor or Data Processing Instructions ("Objection"), then BenchPrep and Customer shall negotiate in good faith to agree to further measures including contractual or operational adjustments relevant to the appointment of the proposed Subprocessor or operation of the Services to address Customer's Objection. Where such further measures cannot be agreed between the parties within forty-five (45) days from BenchPrep's receipt of the Objection (or such greater period agreed by Customer in writing), Customer may by written notice to BenchPrep with immediate effect terminate that part of the Services which require the use of the proposed Subprocessor.

### **6. DATA SUBJECT RIGHTS.**

#### **6.1 BenchPrep shall:**

**6.1.1** upon becoming aware, promptly notify Customer if BenchPrep receives a request from a Data Subject relating to an actionable Data Subject right under any Privacy Law in respect of Personal Data;

**6.1.2** not respond to that request except on the documented instructions of Customer or as required by a Supervisory Authority; and

**6.1.3** upon request from Customer where required by Privacy Laws and in the context of the Services, reasonably assist Customer in dealing with an actionable Data Subject rights request to the extent Customer cannot fulfil this request without BenchPrep's assistance. BenchPrep may fulfil this request by making available functionality that enables Customer to address such Data Subject rights request without additional Processing by BenchPrep. To the extent such functionality is not available, in order for BenchPrep to provide such reasonable assistance, Customer must communicate such request in writing to BenchPrep providing sufficient information to enable BenchPrep to pinpoint and subsequently amend, export or delete the applicable record.

### **7. PERSONAL DATA BREACH.**

**7.1** BenchPrep shall notify Customer without undue delay upon BenchPrep or any Subprocessor confirming a Personal Data Breach, providing Customer with sufficient information to allow Customer to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Privacy Laws. Subject to Section 7.3 below, such notification shall as a minimum:

**7.1.1** describe the nature of the Personal Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;

**7.1.2** communicate the name and contact details of BenchPrep's data protection officer or other relevant contact from whom more information may be obtained;

**7.1.3** describe the likely consequences of the Personal Data Breach in so far as BenchPrep is able to ascertain having regard to the nature of the Services and the Personal Data Breach; and

**7.1.4** describe the measures taken or proposed to be taken to address the Personal Data Breach.

**7.2** BenchPrep shall co-operate with Customer and take such reasonable commercial steps as are necessary to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

**7.3** Where and in so far as, it is not possible to provide the information or BenchPrep is prohibited by law or law enforcement from providing the information referred to in Section 7.1 at the same time, the information may be provided in phases without undue further delay.

### **8. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION.**

**8.1** To the extent necessary, BenchPrep shall provide reasonable assistance to Customer with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Customer reasonably considers to be required by Privacy Laws, in each case solely in relation to Processing of Personal Data by, and taking into account the nature of the Processing and information available to, BenchPrep. To the extent that such impact assessment and/or prior consultation requires assistance beyond BenchPrep providing the applicable BenchPrep processing record(s) and Documentation, BenchPrep shall reserve the right to charge Customer such engagement at BenchPrep's then current daily rates.

### **9. DELETION OR RETURN OF PERSONAL DATA.**

**9.1** Within thirty (30) days from termination or expiry of the Agreement (the "Return Period"), and subject to Section 9.2 below, at Customer's request, BenchPrep will either delete or return available Personal Data. At the expiry of the Return Period, if Customer has not elected either of the foregoing BenchPrep may delete and destroy all Personal Data without notice or liability to Customer. Where Customer requests BenchPrep return available Personal Data, BenchPrep may fulfil this request by making available functionality that enables Customer to retrieve the Personal Data without additional Processing by BenchPrep. If Customer declines to use this functionality, Customer may, within the Return Period, request that BenchPrep return the available Personal Data under an Order for the applicable professional services. In the event the Agreement is terminated for Customer's breach, BenchPrep shall have the right to require that Customer prepay for such professional services. BenchPrep shall provide written confirmation to Customer that it has fully complied with this Section 9 within thirty (30) days of Customer's request for such confirmation.

**9.2** BenchPrep may retain Personal Data to the extent required by Privacy Laws or any other statutory requirement to which BenchPrep is subject and only to the extent and for such period as required by Privacy Laws or any other statutory requirement to which BenchPrep is subject and always provided that (a) during such retention period the provisions of this DPA will continue to apply, (b) that BenchPrep shall ensure the confidentiality of all such Personal Data, and (c) BenchPrep shall ensure that such Personal Data is only Processed as necessary for the purpose(s) specified in the Privacy Laws

requiring its storage or any other statutory requirement to which BenchPrep is subject and for no other purpose.

## **10. REVIEW, AUDIT AND INSPECTION RIGHTS.**

**10.1** Upon Customer's reasonable request, BenchPrep shall provide all relevant and necessary material, documentation and information in relation to BenchPrep's technical and organizational security measures used to protect the Personal Data in relation to the Services provided in order to demonstrate compliance with Privacy Laws.

**10.2** BenchPrep shall ensure a security audit of its technical and organizational security measures is carried out at least annually in compliance with Privacy Laws. The results of such security audit will be documented in a summary report. BenchPrep shall promptly provide Customer upon request with (i) a confidential summary of such report; and (ii) evidence of appropriate remediation of any critical issues within four (4) weeks from date of issuance of the audit report.

**10.3** If, following the completion of the steps set out in Sections 10.1 and 10.2, Customer reasonably believes that BenchPrep is non-compliant with Privacy Laws, Customer may request that BenchPrep make available, either by webinar or in a face-to-face review, extracts of all relevant information necessary to further demonstrate compliance with Privacy Laws. Customer undertaking such review shall give BenchPrep reasonable notice, by contacting BenchPrep's Information Security Director at [privacy@BenchPrep.com](mailto:privacy@BenchPrep.com), and any review will be conducted under this Section 10.3.

**10.4** In the event that Customer reasonably believes that its findings following the steps set out in Section 10.3 do not enable Customer to comply materially with Customer's obligations mandated under the Privacy Laws in relation to its appointment of BenchPrep, then Customer may give BenchPrep not less than thirty (30) days prior written notice of its intention, undertake an audit which may include inspections of BenchPrep to be conducted by Customer or an auditor mandated by Customer (not being a competitor of BenchPrep). Such audit and/or inspection shall (i) be subject to confidentiality obligations agreed between Customer (or its mandated auditor) and BenchPrep, (ii) be undertaken solely to the extent mandated by, and may not be further restricted under applicable Privacy Laws, (iii) not require BenchPrep to compromise the confidentiality of security aspects of its systems and/or data processing facilities (including that of its Subprocessors), and (iv) not be undertaken where it would place BenchPrep in breach of BenchPrep's confidentiality obligations to other BenchPrep customers vendors and/or partners generally or otherwise cause BenchPrep to breach laws applicable to BenchPrep. Customer (or auditor mandated by Customer) undertaking such audit or inspection shall avoid causing any damage, injury or disruption to BenchPrep's premises, equipment, personnel and business in the course of such a review. To the extent that such audit performed in accordance with this Section 10.4 exceeds one (1) business day, BenchPrep shall reserve the right to charge Customer for each additional day at its then current daily rates.

**10.5** If following such an audit or inspection under Section 10.4, Customer, acting reasonably, determines that BenchPrep is non-compliant with Privacy Laws then Customer will provide details thereof to BenchPrep upon receipt of which BenchPrep shall provide its response and to the extent required, a draft remediation plan for the mutual agreement of the parties (such agreement not to be unreasonably withheld or delayed; the mutually agreed plan being the "Remediation Plan"). Where the parties are unable to reach agreement on the Remediation Plan, or in the event of agreement, BenchPrep materially fails to implement the Remediation Plan by the agreed dates which in either case is not cured within forty-five (45) days following Customer's notice or another period as mutually agreed between the Parties, Customer may terminate the Services in part or in whole which relates to the non-compliant Processing and the remaining Services shall otherwise continue unaffected by such termination.

**10.6** The rights of Customer under this Section 10 shall only be exercised once per calendar year unless Customer reasonably believes BenchPrep to be in material breach of its obligations under either this DPA or Privacy Laws.

## **11. RESTRICTED TRANSFERS.**

**11.1** Customer (as "data exporter") and BenchPrep, as appropriate, (as "data importer") hereby agree that the Standard Contractual Clauses shall apply in respect of any Restricted Transfer from Customer to BenchPrep to the extent required by Privacy Laws. The parties agree that signature to this Agreement constitutes all necessary signatures to the Standard Contractual Clauses attached hereto as Annex 2, such that the provisions of the Standard Contractual Clauses shall apply.

**11.2** For the purposes of Annex I or other relevant part of the Standard Contractual Clauses, the Data Processing Instructions sets out the Data Subjects, categories of Personal Data, special categories of Personal Data, Subprocessors and description of Processing (processing operations).

**11.3** For the purposes of Annex II or other relevant part of the Standard Contractual Clauses, the Information Security Schedule sets out the description of the technical and organizational security measures implemented by BenchPrep (the data importer) in accordance with clause 8.6 of the Standard Contractual Clauses.

## **12. OTHER PRIVACY LAWS.**

**12.1** To the extent that Processing relates to Personal Data originating from a jurisdiction or in a jurisdiction which has any mandatory requirements in addition to those in this DPA, both Parties may agree to any additional measures required to ensure compliance with applicable Privacy Laws and any such additional measures agreed to by the Parties will be documented as an Annex to this DPA or in an Order to the Agreement. Due to the fact that BenchPrep has no control over the type, character, properties, content, and/or origin of Personal Data Processed hereunder, notwithstanding anything to the contrary herein, BenchPrep shall not be in breach of this DPA or the Agreement or liable to Customer to the extent Personal Data Subject to jurisdictional requirements mandating security, processing or other measures not set forth in, or contrary to the terms of, this DPA is provided by Customer without amending this DPA or entering into an Order addressing the same.

**12.2** If any variation is required to this DPA as a result of a change in Privacy Laws, including any variation which is required to the Standard Contractual Clauses, then either party may provide written notice to the other party of that change in law. The parties will discuss and negotiate in good faith any necessary variations to this DPA, including the Standard Contractual Clauses, to address such changes.

## **13. GENERAL TERMS.**

**13.1** The parties to this DPA hereby submit to the applicable choice of governing law and jurisdiction stipulated in the Agreement.

**13.2** This DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement. The UN Convention on Contracts for the International Sale of Goods shall not apply in any respect to this Agreement or the parties, regardless of the applicable governing law and jurisdiction.

**13.3** The applicable law provisions of this Agreement are without prejudice to clauses 7 (Mediation and Jurisdiction) and 10 (Governing Law) of the Standard Contractual Clauses where applicable to Restricted Transfers of Personal Data from the European Union (including the United Kingdom) to a third country.

## **14. ORDER OF PRECEDENCE.**

**14.1** Nothing in this DPA reduces BenchPrep's or any BenchPrep Affiliate's obligations under the Agreement in relation to the protection of Personal Data or permits BenchPrep or any BenchPrep Affiliate to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Agreement. In the event of inconsistencies between the provisions of this DPA and (i) the Information Security Schedule, or (ii) any other agreements between the parties, including the Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail.

**15. SEVERANCE.**

**15.1** Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or

unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

**IN WITNESS WHEREOF, Customer and BenchPrep have caused this DPA to be executed by their duly authorized representatives as of the Effective Date.**

**WATERMELON EXPRESS, INC. DBA BENCHPREP**

\_\_\_\_\_  
NAME SIGNED

\_\_\_\_\_  
NAME & TITLE PRINTED

\_\_\_\_\_  
DATE

**COMPANY NAME**  
**CUSTOMER**

\_\_\_\_\_  
NAME SIGNED

\_\_\_\_\_  
NAME & TITLE PRINTED

\_\_\_\_\_  
DATE

**ANNEX 1 TO DPA**  
**DATA PROCESSING INSTRUCTIONS**

**A. LIST OF PARTIES**

If the Standard Contractual Clauses apply, the data exporter(s) and importer(s) are as follows:

<b>Data Exporting Organisation</b>	Name: Customer as identified in the Agreement. Signature and date: By entering into the Agreement, data exporter is deemed to have signed these Standard Contractual Clauses incorporated herein as of the effective date of the Agreement. Role (controller/processor): controller
<b>Data Importing Organisation</b>	Name: Watermelon Express Inc. dba BenchPrep Address: 111 S. Wacker Drive, Suite 1200, Chicago, IL 60606 Signature and date: By entering into the Agreement, data importer is deemed to have signed these Standard Contractual Clauses incorporated herein as of the effective date of the Agreement. Role (controller/processor): processor

**B. DESCRIPTION OF TRANSFER**

<b>Processing Activity: Support</b>	Support may be provided by BenchPrep in accordance with BenchPrep's Support Plan. When providing Support, BenchPrep may be required by Customer to Process Personal Data. BenchPrep may access and/or receive Personal Data when providing Support.  Personal Data is not accessed and/or received in every Support case because some errors can be analyzed and rectified without such access if the background to the error is known. Depending on the issue, BenchPrep or third-party vendors may provide Support and therefore an international transfer of Personal Data may occur.
<b>Processing Activity: Professional Services</b>	If, as part of an Order, Customer requires BenchPrep to perform Professional Services to assist in deployment of the product during the term, then BenchPrep may be required by Customer to Process Personal Data as part of this engagement.
<b>Processing Activity: Hosted Subscription Services</b>	Customer will upload data to the Hosted Subscription Services in order to maximize the functionality of the product. Some of the data which may be uploaded to the Hosted Subscription Services may include Personal Data. BenchPrep will store (either directly or using a third party Subprocessor as noted below) all data uploaded into the Hosted Subscription Services on behalf of Customer in accordance with the terms and conditions of service under the Agreement as mutually agreed to by the Parties.  Customer will determine how and why the product will be used to its benefit which may include the frequent or infrequent use of Personal Data. Customer acknowledges that in relation to these Processing operations, BenchPrep has no control over the submission of Data Subject's Personal Data and that the design of the data to be submitted to BenchPrep's Hosted Subscription Services is at all times under the control of Customer. Except for the storage of the data within the Hosted Subscription Services (and the provision of Support, if applicable, described above), BenchPrep is not involved in any Processing activities associated with this use of the product. If, as part of an Order, Customer requires BenchPrep to perform Professional Services to assist in deployment of the product or application managed services during the Term, then BenchPrep may be required by Customer to Process Personal Data for those purposes.
<b>Categories of Personal Data</b>	<ul style="list-style-type: none"> <li>Customer's employee categories: name, title, department, ID number, system usage, email address, job title, login credentials and/or contact telephone number.</li> <li>Customer's end-user or consumer categories: name, email address, contact telephone number, account number. Additional Categories of Personal Data may be provided by Customer either as part of a Support request or through Customer's use of Hosted Subscription Services.</li> </ul>
<b>Special Categories of Personal Data</b>	Not applicable.
<b>Data Subjects</b>	Employees, clients, customers and suppliers of Customer. Employees or contractors of Customer who contact BenchPrep's technical support facilities.
<b>Duration of Processing</b>	<u>Support &amp; Professional Services</u> : Personal Data is processed only for as long as is necessary to provide the particular Support and/or Professional Services. <u>SaaS</u> : Personal Data is stored for the duration of the Services and is deleted or returned to Customer as set out in the data processing agreement or as otherwise amended or deleted by Customer during the Access Term.

**C. COMPETENT SUPERVISORY AUTHORITY**

<b>COMPETENT SUPERVISORY AUTHORITY</b>	The Data Protection Commission (DPC) ( <a href="https://www.dataprotection.ie/en">https://www.dataprotection.ie/en</a> )
--	--

#### D. THIRD PARTY SUBPROCESSORS

Subprocessor Name	Location	Services Provided
Amazon Web Services	USA	CDN and S3 Services
IBM	USA	Cloud Platform
Pendo.io	USA	User Guides
Google G-Suite	USA	Email, File Storage, etc.
DropBox	USA	File Storage
Slack	USA	Communication
Airbrake.io	USA	Exception Monitoring
HappyFox	USA	Ticket Support Tool
Zencoder	USA	Video Encoding
Mailgun	USA	Email Tool
Jira/Confluence	USA	Product/Project Management
Salesforce	USA	Customer Relationship Management
BigCommerce	USA	e-commerce solution
Domo	USA	Reporting & Data Visualization
Snowflake	USA	Data Warehouse
Sisense	USA	Reporting and Business Intelligence
Linksquares	USA	Contract Lifecycle Management Software
Fivetran	USA	Data Integration
NewRelic	USA	Application & Infrastructure Performance & Monitoring

## **ANNEX 2: STANDARD CONTRACTUAL CLAUSES (PROCESSORS)**

### **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) <sup>(1)</sup> for the transfer of 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<sup>1</sup> (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 'Vendor')  
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 Vendor, with the following exceptions:
- (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
- (ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);
- (iii) Clause 9(a), (c), (d) and (e);
- (iv) Clause 12(a), (d) and (f);
- (v) Clause 13;
- (vi) Clause 15.1(c), (d) and (e);
- (vii) Clause 16(e);
- (viii) Clause 18(a) and (b).
- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

#### **Clause 4 Interpretation**

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

---

<sup>1</sup> Annex 1 to Schedule E of the DPA serves as Annex I to the Standard Contractual Clauses. Schedule D of the Master Services Agreement serves as Annex II to the Standard Contractual Clauses.

(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**

N/A

### **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 Vendor is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

##### **8.1 Instructions**

- (a) The Vendor 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 Vendor shall immediately inform the data exporter if it is unable to follow those instructions.

##### **8.2 Purpose limitation**

The Vendor 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 Vendor 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 Vendor 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 Vendor shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the Vendor 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 Vendor shall continue to ensure compliance with these Clauses. In case of local laws applicable to the Vendor that prohibit return or deletion of the personal data, the Vendor 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 Vendor 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 Vendor 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 Vendor shall at least implement the technical and organisational measures specified in Annex II. The Vendor shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- (b) The Vendor 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 Vendor under these Clauses, the Vendor shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The Vendor 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 Vendor 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 Vendor.

## 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 Vendor shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

## 8.8 Onward transfers

The Vendor 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 Vendor 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 Vendor with all the other safeguards under these Clauses, in particular purpose limitation.

## 8.9 Documentation and compliance

- (a) The Vendor 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 Vendor shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- (c) The Vendor 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 Vendor.
- (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 Vendor 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 thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the Vendor 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 Vendor under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the Vendor fulfils its obligations under Clause 8.8. The Vendor shall ensure that the sub-processor complies with the obligations to which the Vendor is subject pursuant to these Clauses.

(c) The Vendor 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 Vendor may redact the text of the agreement prior to sharing a copy.

(d) The Vendor shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the Vendor. The Vendor shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The Vendor shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the Vendor 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 Vendor 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 Vendor 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 Vendor shall comply with the instructions from the data exporter.

#### **Clause 11** **Redress**

(a) The Vendor 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 Vendor 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 Vendor shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The Vendor 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 Vendor 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 Vendor 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 Vendor (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 Vendor (or its sub-processor), it shall be entitled to claim back from the Vendor that part of the compensation corresponding to the Vendor'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 Vendor may not invoke the conduct of a sub-processor to avoid its own liability.

### **Clause 13**

#### **Supervision**

- (a) 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 Vendor 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 Vendor 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 Vendor, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the Vendor 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 Vendor 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 Vendor 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 Vendor 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 Vendor 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 Vendor in case of access by public authorities**

#### **15.1 Notification**

- (a) The Vendor 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 Vendor is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the Vendor 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 Vendor 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 Vendor 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 Vendor 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 Vendor 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 Vendor 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 Vendor shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the Vendor 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 Vendor under Clause 14(e).
- (b) The Vendor 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 Vendor 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 Vendor shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the Vendor 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 Vendor 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 Vendor 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 Vendor is in substantial or persistent breach of these Clauses; or
- (iii) the Vendor 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 Vendor shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the Vendor shall continue to ensure compliance with these Clauses. In case of local laws applicable to the Vendor that prohibit the return or deletion of the transferred personal data, the Vendor 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 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 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 Vendor 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.
-