# MALBEK DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") forms is hereby incorporated under the [INSERT MASTER AGREEMENT TITLE] (collectively the "**Agreement**") entered into by and between [INSERT CUSTOMER] ("**Customer**" or "**Controller**") and Malbec Solutions, Inc. d/b/a Malbek ("**Vendor**" or "**Processor**"). Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement.

## HOW THIS DPA APPLIES

The terms of this DPA only apply to Customer and Vendor as follows:

A. Sections 1 through 8, Attachment 1, Appendix 1, and Appendix 2 apply when Data Protection Laws and Regulations apply to the Agreement.
B. When only the California Consumer Privacy Act ("**CCPA**") applies to the Agreement, then only Section 8 and Appendix 3 apply.
C. The entire DPA along with all appendices and attachments apply when Data Protection Laws and Regulations and the CCPA apply to the Agreement.

## 1. DEFINITIONS

Any capitalized terms not defined herein shall have the meaning given to that term in the Agreement, CCPA, or Data Protection Laws and Regulations.

**"Data Controller"** means the entity which determines the purposes and means of the Processing of Personal Data.

**"Data Processor"** means the entity which Processes Personal Data on behalf of the Data Controller.

**"Data Protection Laws and Regulations"** means all laws and regulations, including EU General Data Protection Regulation (GDPR), laws and regulations of the European Union, the European Economic Area ("**EEA**") and their member states, Switzerland and the United Kingdom, applicable to the Processing of Personal Data with the Service under the Agreement.

**"Data Subject"** means the individual to whom Personal Data relates.

**"Personal Data"** means any information (i) of an identified or identifiable person and, (ii) of an identified or identifiable legal entity (where protected under applicable Data Protection Laws and Regulations), where such data is submitted to the Service.

**"Processing"** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

**"Service"** means as defined in the Agreement or the software as a service applications provided by Vendor to which Customer is licensed to use.

**"Subprocessor"** means any third party appointed by or on behalf of Vendor to Process Personal Data in connection with the Service.

## 2. PROCESSING OF PERSONAL DATA

**2.1 Roles of the Parties.** The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Data Controller and Vendor is a Data Processor.

**2.2 Customer's Responsibilities**. Customer shall, in Customer's use of the Service, submit or make available Personal Data to Vendor for Processing in accordance with the requirements of Data Protection Laws and Regulations, and Customer's instructions to Vendor for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the initial accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. Notwithstanding anything to the contrary, Customer agrees that is solely responsible for (i) configuring all Vendor-provided software features as necessary for Customer to use and process Personal Data in compliance with applicable law, including Data Protection Legislation and the CCPA; and (ii) implementing and following any Vendor-provided requirements relating to such compliance.

**2.3 Customer's Instructions**. Vendor shall only Process Personal Data on behalf of and in accordance with Data Protection Laws and Regulations, Customer's instructions, and as authorized under the Agreement (including as is necessary to provide the Service), and shall treat Personal Data as Confidential Information. Customer instructs Vendor to Process Personal Data for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s), including to provide you the Service; (ii) Processing initiated by Users in their use of the Service; and (iii)

Processing to comply with other reasonable instructions provided by Customer (e.g., via email). Vendor will notify Customer upon becoming aware and if in Vendor's reasonable judgement that Customer's instruction violates Data Protection Laws and Regulations.

## 3. RIGHTS OF DATA SUBJECTS

**3.1 Correction, Blocking, and Deletion.** To the extent Customer, in Customer's use of the Service, does not have the ability to correct, amend, block or delete Personal Data, as required by Data Protection Laws and Regulations, Vendor shall assist Customer in facilitating such actions to the extent Vendor is legally permitted to do so.

**3.2 Data Subject Requests.** Vendor shall, to the extent legally permitted, notify Customer without undue delay if Vendor receives a request from a Data Subject for access to, correction, amendment or deletion of that Data Subject's Personal Data. If legally permitted, Vendor shall not respond to any such Data Subject request without Customer's prior written consent except to confirm that the request relates to Customer. Vendor shall cooperate and assist in relation to the handling of a Data Subject's request for access to that person's Personal Data, to the extent legally permitted and to the extent Customer does not have access to such Personal Data through use of the Service.

## 4. VENDOR PERSONNEL

**4.1 Confidentiality.** Vendor shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. Vendor shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

**4.2 Limitation of Access.** Vendor shall ensure that Vendor's access to Personal Data is limited to those personnel who require such access to perform under the Agreement.

## 5. SECURITY

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, Vendor shall implement appropriate technical and organizational measures designed to ensure a level of security appropriate to the risk and as detailed in Appendix 2. Vendor regularly monitors compliance with these safeguards. Vendor may update these technical and organization measures from time to time, but will not materially decrease the overall security of the Service.

## 6. SECURITY BREACH MANAGEMENT AND NOTIFICATION

Vendor maintains security incident management policies and procedures and shall, to the extent permitted by law, without undue delay, notify Customer of any actual unauthorized access, use, modification, or disclosure of Personal Data, by Vendor or its Subprocessors (a "**Security Breach**"). Vendor shall make all reasonable efforts to identify and take all reasonable steps to remediate the cause of such Security Breach.

## 7. SUBPROCESSORS

**7.1 Subprocessors.** Pursuant to this DPA and Clause 5(h) of the Standard Contractual Clauses (if applicable), Customer acknowledges and expressly agrees that Vendor is granted the authority to subcontract the processing of Personal Data to Subprocessors provided that:

**7.1.1** Vendor or Vendor affiliates on its behalf may engage Subprocessors under a written (including in electronic form) contract consistent with the terms of this DPA in relation to the Subprocessor's processing of Personal Data. Vendor shall be liable for any breaches by the Subprocessor in accordance with the terms of this DPA.

**7.1.2** Vendor will evaluate the security, privacy and confidentiality practices of a Subprocessor prior to selection to establish that it is capable of providing the level of protection of Personal Data required by this DPA.

**7.1.3** Vendor will provide a list of subprocessors including the name, geographic location, and role of each Subprocessor.

**7.1.4** Vendor will inform Customer in writing and in advance of any intended additions or replacements to the list of Subprocessors including name, address and role of the new Subprocessor. Customer can object to any new subprocessor provided that a legitimate reason is provided under appliable data protection laws including but not limited to the General Data Protection Regulation. Within 30 days from the date of Vendor's notice to Customer informing Customer of the new Subprocessor, Customer may request that the parties discuss in good faith a resolution to the objection. Such discussions shall not affect Vendor's right to use the new Subprocessor(s) after 30 days.

**7.1.5** Vendor may replace a Subprocessor without advance notice where the reason for the change is outside of

Vendor's reasonable control and prompt replacement is required for security or other urgent reasons. If this occurs, Vendor will inform Customer of the replacement Subprocessor as soon as possible following its appointment.

## 8. ADDITIONAL TERMS

**8.1 Application of Standard Contractual Clauses.** The Standard Contractual Clauses in Attachment 1 and the additional terms in this Section 8 will apply to the Processing of Personal Data by Vendor in the course of providing Services as follows:

**8.1.1** Notwithstanding anything to the contrary in this DPA, the Standard Contractual Clauses apply only to Personal Data that is transferred from the EEA and/or Switzerland and the United Kingdom to outside the EEA and Switzerland or the United Kingdom, either directly or via onward transfer, to any country or recipient: (i) not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the EU Data Protection Directive or its successors), and (ii) not covered by a suitable framework (e.g. Binding Corporate Rules for Processors, etc.) recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data. In the event the United Kingdom is no longer considered or effectively part of the EU or EEA then such transfers of Personal

Data to and from the United Kingdom will be treated as a non-EU or EEA country and the terms of this Section 8.1.1 will apply accordingly.

**8.1.2** Subject to Section 8.1.1, the Standard Contractual Clauses apply to (i) the legal entity that has executed the Agreement and is the Data Exporter and, (ii) all Affiliates (as defined in the Agreement) of Customer established within the EEA and Switzerland or the United Kingdom that have licensed the Service. For the purpose of the Standard Contractual Clauses and this Section 7, the aforementioned entities shall be deemed "Data Exporters".

**8.2 Objective and Duration.** The objective of Processing of Personal Data by Vendor is the provision of the Service pursuant to the Agreement for the term(s) of the Agreement. Vendor shall process Customer Data solely for the following purposes:

**8.2.1** Product improvement (in particular, product features and functionality, workflows and user interfaces) and development of new Delighted products and services,

**8.2.2** improving product performance,

**8.2.3** Internal support resource demand allocation and planning.

**8.3 Audits.** Vendor shall make available to Customer all information necessary to reasonably demonstrate compliance with this DPA, and shall allow for and contribute to audits, including inspections in relation to the Processing of the Personal Data by the Vendor. Such audits and inspections may be conducted by an third party auditor, provided that such third-party auditor shall be subject to confidentiality obligations and provided that such audits and inspections and the results therefrom, including the documents reflecting the outcome of the audit and/or the inspections, shall only be used by Customer to assess compliance with this DPA, and shall not be used for any other purpose or disclosed to any third party without Vendor's prior written approval. Upon Vendor's first request, Customer shall return all records or documentation in Customer's possession or control provided by Vendor in the context of the audit and/or the inspection. Notwithstanding anything to the contrary, (i) Customer shall give Vendor reasonable prior written notice of at least fourteen (14) days of any audit or inspection to be conducted by it; (ii) Customer's right to conduct any audit under this DPA shall be limited to once per twelve (12) month period except where required by law or in the event of Vendor's breach of this DPA; and (iii) all audits shall occur during Vendor's normal business hours without undue disruption to Vendor's business.

**8.4 Return and Deletion of Personal Data.** Where applicable based on the Service, Vendor will return and delete Personal Data in accordance with the Agreement. Customer is responsible for the correction, amendment, blocking or deleting of Personal Data within its control within the Service. Vendor will provide reasonable assistance to Customer in the correcting, amendment, blocking or deleting of Personal Data in the Service.

**8.5 Privacy Impact Assessment and Prior Consultation.** Taking into account the nature of the Services and the information available to Vendor, Vendor will provide commercially reasonable assistance to Customer in complying with Customer's obligations in respect of data protection impact assessments and prior consultation pursuant to Articles 35 and 36 of the GDPR.

## 9. OTHER

**9.1** This DPA and liability or remedies arising hereunder are subject to any and all limitations on liability and disclaimers of types of damages in the Agreement. This DPA automatically terminates upon termination or expiration of the Agreement.

**9.2** Subject to applicability in accordance with Section 7.1, in the event of any conflict or inconsistency between this DPA and the Agreement on the one hand and the Standard Contractual Clauses in Attachment 1 on the other hand, the Standard Contractual Clauses shall prevail.

**9.3** Notices under the DPA and the Standard Contractual Clauses shall be in accordance with the Agreement.

# ATTACHMENT 1

## Standard Contractual Clauses for Personal Data Transfers from an EU Controller to a Processor Established in a Third Country (Controller-to-Processor Transfers)

### 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 - Optional**

**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 thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

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

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

## 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 established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a

representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose 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 XXX.

## 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 XXX

(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.

# ANNEX I

## A. LIST OF PARTIES

**Data exporter(s):** [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*]

1. Name: …

Address: …

Contact person's name, position and contact details: …

Activities relevant to the data transferred under these Clauses: …

Signature and date: …

Role (controller/processor): Controller

**Data importer(s):** [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection*]

1. Name: Malbec Solutions, Inc. d/b/a Malbek

Address: Address: 300 Carnegie Center, Suite 210, Princeton NJ 08540

Contact person's name, position and contact details: Matt Patel, COO, matt@malbek.io

Activities relevant to the data transferred under these Clauses: Malbek is a provider of contract lifecycle management software and services for its customers (the Data exporters).

Signature and date: …

Role (controller/processor): Processor

## B. DESCRIPTION OF TRANSFER

*Categories of data subjects whose personal data is transferred*

Data Exporter may submit Personal Data to the Service, the extent of which is determined and controlled solely by the Data Exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects:

- Data Exporter's agents, including employees and officers
- Data Exporter's client's agents, including employees and officers

Categories of personal data transferred

The Personal Data transferred concern the following categories of data (please specify):

Data Exporter may submit Personal Data to the Service, the extent of which is determined and controlled solely by the Data Exporter in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Employment title
- Position
- Email address

- IP address
- Telephone number
- Contract data

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

None

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

Data Exporter will have the ability to continuously transfer data to Data Importer throughout the term of the Agreement.

*Nature of the processing*

Storage and use of data as necessary to provide the Data Importer with contract lifecycle management software and services.

*Purpose(s) of the data transfer and further processing*

The objective of processing of Personal Data by Data Importer is the performance of the Service and support services pursuant to the Agreement.

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

Duration of the Service and 30 days beyond the termination of the Service.

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

None

**C. COMPETENT SUPERVISORY AUTHORITY**

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

## ANNEX II

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

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

*Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.*

Data Importer shall implement appropriate and commercially reasonable physical, technical and organizational measures designed to ensure that data exporter's and its clients' personal data is protected against accidental, unauthorized or unlawful use, processing, destruction, loss, disclosure or access. The technical and organizational measures shall ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation, the nature and scope, context and purpose of processing and risks of varying likelihood and severity for the rights and freedoms of individuals. These measures shall include, as appropriate, (a) encryption and pseudonymization of personal data, (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing; and (e) establishing measures to identify vulnerabilities with regard to the processing of personal data in systems used to provide the services to the Data Exporter.

Data Importer will not materially decrease the overall level of the above technical and security measures during term of the underlying agreement, term of use, license and/or subscription term

*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 data exporter*

## ANNEX III

### LIST OF SUB-PROCESSORS

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

Sub Processors can be found here: https://www.malbek.io/sub-processors

Contact Person: details: Matt Patel, COO, matt@malbek.io

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): …

2. Storage of data and allow for processing of data to provide the Services as per the Agreement.

# APPENDIX 3 TO THE DPA

Words and phrases defined in the CCPA shall have the same meaning in this Appendix and all other terms shall have the meaning in the Agreement. In the event of a conflict between the terms of this Appendix and the Agreement, this Appendix will control but all other terms in the Agreement will otherwise remain in full force.

**1. The following definitions and rules of interpretation apply in this Appendix:**

(a) CCPA means the California Consumer Privacy Act of 2018, (Cal. Civ. Code §§ 1798.100 to 1798.199), and any related regulations provided by the California Attorney General all of which as may be amended from time to time.

(b) Contracted Business Purposes means the Services and as otherwise described in the Agreement for which the Vendor receives or accesses personal information from Customer.

**2. Vendor's CCPA Obligations:**

(a) Vendor will only collect, use, retain, or disclose personal information for the Contracted Business Purposes for which Customer provides or permits personal information access.

(b) Vendor will not collect, use, retain, disclose, sell, or otherwise make personal information available in a way that does not comply with the CCPA. If a law requires Vendor to disclose personal information for a purpose unrelated to the Contracted Business Purpose, Vendor must first inform the Customer of the legal requirement and give the Customer an opportunity to object or challenge the requirement, unless applicable law prohibits such notice.

(c) To the extent commercially reasonable, Vendor will limit personal information collection, use, retention, and disclosure to activities reasonably necessary and proportionate to achieve the Contracted Business Purposes or another compatible operational purpose.

(d) Vendor must promptly comply with any Customer request or instruction requiring the Vendor to provide, amend, transfer, or delete the personal information, or to stop, mitigate, or remedy any unauthorized processing. If Customer is able to amend, transfer, or delete the personal information itself and chooses Vendor’s assistance, Customer agrees to pay reasonable fees for such assistance at a rate mutually agreed in advance between the parties.

(e) If the Contracted Business Purposes require the collection of personal information from individuals on the Customer's behalf, Vendor will always provide a CCPA-compliant notice addressing use and collection methods.

(f) If the CCPA permits, Vendor may aggregate, deidentify, or anonymize personal information, so it no longer meets the personal information definition, and may use such aggregated, deidentified, or anonymized data for its own research and development purposes. Vendor will not attempt to or actually re-identify any previously aggregated, deidentified, or anonymized data and will contractually prohibit downstream data recipients from attempting to or actually re-identifying such data.

**3. Assistance with CCPA Obligations:**

(a) Vendor will reasonably cooperate and assist Customer in responding to CCPA-related inquiries, including responding to verifiable consumer requests, taking into account the nature of Vendor's processing and the information available Vendor.

(b) A party must notify the other party promptly if it receives any complaint, notice, or communication that directly or indirectly relates to either party's compliance with the CCPA. Specifically, Vendor must notify the Customer within five (5) working days if it receives a verifiable consumer request under the CCPA.

**4. Subcontracting:**

(a) Vendor may use subcontractors to provide the Contracted Business Services. Vendor cannot make any disclosures to the subcontractor that the CCPA would treat as a sale and Vendor shall ensure appropriate terms no less protective than those in this Appendix are entered into between Vendor and the subcontractor.

(b) Vendor remains fully liable for each subcontractor's performance to the same extent if Vendor were performing itself.

(c) Upon the Customer's written request, Vendor will provide Customer with information and reports demonstrating Vendor’s compliance with the obligations in this Appendix.

**5. Certifications:**

(a) Both parties will comply with all applicable requirements of the CCPA when collecting, using, retaining, or disclosing personal information.

(b) Vendor certifies that it understands this Appendix’s and the CCPA's restrictions and prohibitions on selling personal information and retaining, using, or disclosing personal information outside of the parties' business relationship, and Vendor will comply with them.