

## Data Processing Agreement for Resellers/Distributors/Partners

### Incorporating the Standard Contractual Clauses: Controller to Processor Transfer

This Data Processing Agreement for Resellers, Distributors and Partners ("**DPA**") is incorporated by reference into the terms of any existing and current agreement (the "**Agreement**") between Idera, Inc. ("**Idera**") or each Affiliate of Idera listed in the attached Exhibit A, which Idera is acting on behalf, including, but not limited to, the extent they are considered data exporters under the Standard Contractual Clauses 2010 (each an "**Idera Affiliate**") and the counterparty agreeing to these terms ("**Partner**") under which Partner agrees to provide Idera or Idera Affiliate with certain services (the "**Services**") described in the Agreement. All capitalized terms that are not expressly defined in this DPA will have the meanings given to them in the Agreement. The term Partner, Distributor and Reseller shall be used interchangeably solely for purpose of this DPA.

#### 1. DEFINITIONS

"**Affiliate**" means any entity that, directly or indirectly, controls, is controlled by or is under common control with Idera, where "control" is defined as the ownership of at least fifty percent (50%) of the equity or beneficial interests of such entity.

"**Personal Data**", "**special categories of data**", "**process/processing**", "**Controller**", "**Processor**", "**Data Subject**" and "**supervisory authority**" shall have the same meaning as in the Regulation.

"**C-to-P Transfer Clauses**" means the Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries approved by EC Commission Decision of 5 February 2010 as set out in Schedule 1 to this DPA.

"**Data Protection Laws**" means the Regulation, the Data Protection Act 1998, any successor thereto, and any applicable European Union or Member State law relating to the data protection or privacy of individuals.

"**Idera Affiliate**" has the meaning ascribed to such term in the Preamble hereto.

"**Regulation**" means Directive 95/46, and any subsequent regulation, including Regulation (EU) 2016/679 of the European Parliament and the Council (General Data Protection Regulation).

"**Regulator**" means the data protection supervisory authority which has jurisdiction over the Idera's or Partner's processing of Personal Data.

"**Subprocessor**" means any processor engaged by the Partner or by any other subprocessor of the Partner, which agrees to receive from the Partner, or from any other subprocessor of the Partner, Idera Personal Data exclusively with the intention for processing activities to be carried out on behalf of the Idera or an Idera Affiliate and in accordance with its instructions, the terms of the Agreement, the DPA and the terms of the written subcontract.

#### 2. DETAILS OF THE PROCESSING ACTIVITIES

- 2.1 Idera or, where applicable, an Idera Affiliate shall be the Controller and Partner shall be the Processor regarding the Personal Data processed by Partner on Idera's or an Idera Affiliate's behalf ("**Idera Personal Data**") under the Agreement.
- 2.2 The details of the processing activities to be carried out by the Partner on behalf of the Idera or, where applicable, an Idera Affiliate under the Agreement and in particular the special categories of data where applicable, are specified in Appendix 1 of Schedule 1.

#### 3. OBLIGATIONS OF THE PARTNER

The Partner agrees and warrants:

- 3.1 to process Idera Personal Data only:
  - (a) on behalf of Idera or, where applicable, an Idera Affiliate and in accordance with its documented instructions unless otherwise required by European Union or European Member State law to which the Partner is subject;
  - (b) for the sole purpose of carrying out the Services or as otherwise instructed by Idera or, where applicable, an Idera Affiliate, and not for the Partner's own purposes or other commercial exploitation except in the legitimate

interest of the Partner, in accordance with section 6.f of the GDPR, or any other applicable Data Protection Laws. This provision shall not apply to anonymized DDoS and traffic statistics that may be collected as long as such data cannot be attributed directly or in combination with other data to Idera's Personal Data; and

- (c) in compliance with this DPA; and
  - (d) in an encrypted and anonymized manner as necessary while in transit and storage and in accordance with the current state of the art encryption technology as available in the commercial marketplace
- 3.2 if it is legally required to process Idera Personal Data otherwise than as instructed by Idera or, where applicable, an Idera Affiliate, Partner shall notify Idera or, where applicable, an Idera Affiliate before such processing occurs, unless the Data Protection Law requiring such processing prohibits the Partner from notifying Idera or, where applicable, an Idera Affiliate on an important ground of public interest, in which case it shall notify Idera or, where applicable, an Idera Affiliate as soon as that Data Protection Law permits it to do so.
- 3.3 that it has implemented and will maintain appropriate technical and organisational measures in accordance with those described in International Organization for Standardization (ISO 27001, ISO 27018 or its equivalent or superseding standard if applicable) to protect Idera Personal Data against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access and, in particular, where the processing involves the transmission of data over a network, against all other unlawful forms of processing. Having regard to the state of the art and cost of their implementation, the Partner agrees that such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of Idera Personal Data to be protected and will at a minimum include those measures described in Appendix 2 of Schedule 1.
- 3.4 that protective devices are set up for ensuring the integrity and the authenticity of Idera's Personal Data, especially the state of the art protective devices against malware and similar security attacks.
- 3.5 that it has implemented measures to prevent Idera Personal Data from undergoing any unwanted degradation or deletion without having a copy immediately usable;
- 3.6 that it has a business continuity plan which includes measures to reduce unavailability of the services in the event of a lasting incident or security breach, and which includes service levels and maximum recovery response and resolution time charter to face any crisis scenario;
- 3.7 that it will treat all Idera Personal Data as confidential information and not disclose such confidential information without Idera's or, where applicable, an Idera Affiliate's prior written consent except:
- (a) to those of its personnel who need to know the confidential information in order to carry out the Services; and
  - (b) where it is required by a court to disclose Idera Personal Data, or there is a statutory obligation to do so, but only to the minimum extent necessary to comply with such court order or statutory obligation.
- 3.8 to take reasonable steps to ensure that its personnel who have access to the Personal Data:
- (a) are subject to a Code of conduct and an Ethic Guide substantially compliant with Idera's or, where applicable, an Idera Affiliate's Code of Conduct available upon request;
  - (b) are both informed of the confidential nature of the Idera Personal Data and obliged to keep such Idera Personal Data confidential; and
  - (c) are aware of and comply with the Partner's duties and their personal duties and obligations under this DPA.
- 3.9 that it will promptly, and at least within 24 hours, notify Idera about:
- (a) any instruction which, in its opinion, infringes applicable law;

- (b) any actual or suspected security breach, unauthorised access, misappropriation, loss, damage or other compromise of the security, confidentiality, or integrity of Idera Personal Data processed by Partner or a subprocessor ("**Security Breach**");
- (c) any complaint, communication or request received directly by the Partner or a subprocessor from a Data Subject and pertaining to their Personal Data, without responding to that request unless it has been otherwise authorised to do so by Idera; and
- (d) any change in legislation applicable to the Partner or a subprocessor which is likely to have a substantial adverse effect on the warranties and obligations in this DPA.

3.10 that upon discovery of any Security Breach, it shall:

- (a) immediately take action to prevent any further Security Breach; and
- (b) provide Idera or, where applicable, an Idera Affiliate with full and prompt cooperation and assistance in relation to any notifications that Idera or, where applicable, an Idera Affiliate is required to make as a result of the Security Breach.

3.11 to provide Idera or, where applicable, an Idera Affiliate with full and prompt cooperation and assistance in relation to any complaint, communication or request received from a Data Subject, including by:

- (a) providing Idera or, where applicable, an Idera Affiliate with full details of the complaint, communication or request;
- (b) where authorized by Idera or, where applicable, an Idera Affiliate, complying with a request from a Data Subject in relation to their Idera Personal Data within the relevant timescales set out by applicable law and in accordance with Idera's or, where applicable, an Idera Affiliate's instructions;
- (c) providing Idera or, where applicable, an Idera Affiliate with any Idera Personal Data it holds in relation to a Data Subject, if required in a commonly-used, structured, electronic and machine-readable format;
- (d) providing Idera or, where applicable, an Idera Affiliate with any information requested by Idera relating to the processing of Idera Personal Data under this DPA;
- (e) correcting, deleting or blocking any Idera Personal Data; and
- (f) implementing appropriate technical and organisational measures that enable it to comply with this paragraph 3.10.

3.12 to provide Idera or, where applicable, an Idera Affiliate with full and prompt cooperation and assistance in relation to any data protection impact assessment or regulatory consultation that Idera or, where applicable, an Idera Affiliate is legally required to make in respect of Idera Personal Data.

3.13 to appoint, and identify to Idera or, where applicable, an Idera Affiliate, an individual to support the Idera or, where applicable, an Idera Affiliate in monitoring compliance with this DPA, and to make available to Idera or, where applicable, an Idera Affiliate upon request all information and evidence necessary to demonstrate that the Partner is complying with its obligations under this DPA.

3.14 at the request of Idera or, where applicable, an Idera Affiliate, to submit its data processing facilities for audits and inspections of the processing activities covered by this DPA, which shall be carried out by Idera or, where applicable, an Idera Affiliate or any independent or impartial inspection agents or auditors selected by Idera or, where applicable, an Idera Affiliate and not reasonably objected to by the Partner.

3.15 that it shall maintain a list of subprocessors that may Process the Personal Data of Partner's, and make available such list to Idera or, where applicable, an Idera Affiliate. Partner shall require all subprocessors to abide by substantially the same obligations as Partner under this Agreement. Partner remains responsible at all times for compliance with the terms of this Agreement by Partner Affiliates and subprocessors. Idera or, where applicable,

an Idera Affiliate consents to Partner's use of Partner's Affiliates and subprocessors in the performance of the Services. Partner shall inform Idera or, where applicable, an Idera Affiliate of any new subprocessors Partner intends to engage. Idera or, where applicable, an Idera Affiliate may object to the engagement of any new subprocessor, but shall not unreasonably withhold its consent to such appointment.

3.16 upon request, to promptly send a copy of any data privacy, data protection (including but not limited to measures and certifications) and confidentiality portions of an agreement it concludes with a subprocessor relating to Idera Personal Data to Idera or, where applicable, an Idera Affiliate.

3.17 shall promptly notify Idera or, where applicable, an Idera Affiliate should Partner receive a request from a data subject to have access to Personal Data or any complaint or request relating to Idera's or, where applicable, an Idera Affiliate's obligations under applicable Data Protection Laws. Idera or, where applicable, an Idera Affiliate is solely responsible for responding to such request unless Partner does not inform Idera or, where applicable, an Idera Affiliate of the request, and Partner will not respond to any such data subject unless required by applicable laws or unless instructed in writing by Idera or, where applicable, an Idera Affiliate to do so.

#### **4. LIABILITY**

4.1 The Partner shall remain fully liable to Idera or, where applicable, an Idera Affiliate for any subprocessors' processing of Idera Personal Data under the Agreement.

#### **5. INTERNATIONAL DATA TRANSFER**

5.1 Without prejudice to any applicable Data Protection laws, no international transfer of Personal Data may take place to countries that do not provide for an adequate level of protection. Additionally, Personal Data processed within the European Economic Area (the "EEA") by Partner pursuant to the Agreement shall not be exported outside the EEA without the prior written permission of Idera or, where applicable, an Idera Affiliate.

5.2 Where Partner has obtained Idera's or, where applicable, an Idera Affiliate's prior written permission to the transfer in accordance with clause 5.1, the Partner agrees to comply with all applicable Data Protection Laws, and where relevant, the C-to-P Transfer Clauses in its capacity as the processor whereby the Idera or, where applicable, an Idera Affiliate will be regarded as the Data Exporter and the Partner will be regarded as the Data Importer.

5.3 The C-to-P Transfer Clauses may be varied or terminated only as specifically set out in the C-to-P Transfer Clauses.

5.4 In the event of inconsistencies between the provisions of the C-to-P Transfer Clauses and this DPA or other agreements between the parties, the C-to-P Transfer Clauses shall take precedence. In the event that the C-to-P Transfer Clauses are amended, replaced or repealed by the European Commission or under Data Protection Laws, the parties shall work together in good faith to enter into any updated version of the C-to-P Transfer Clauses or negotiate in good faith a solution to enable a transfer of Personal Data to be conducted in compliance with Data Protection Laws.

#### **6. INDEMNITY**

6.1 The Partner agrees to indemnify and defend at its own expense Idera or, where applicable, an Idera Affiliate against all costs, claims, losses, damages or expenses incurred by Idera or, where applicable, an Idera Affiliate or for which Idera or, where applicable, an Idera Affiliate may become liable due to any failure by the Partner or its employees or agents to comply with any of its obligations under this DPA.

#### **7. ALLOCATION OF COSTS**

7.1 Each party shall perform its obligations under this DPA at its own cost.

8. **TERM AND TERMINATION OF THE SERVICES**

- 8.1 The parties agree that Idera Personal Data will be processed by the Partner for the duration of the Services under the Agreement.
- 8.2 The parties agree that upon termination of the Services in so far as they relate to Idera Personal Data, the Partner and all subprocessors shall, at the choice of Idera or, where applicable, an Idera Affiliate, return all Idera Personal Data and the copies thereof to Idera or, where applicable, an Idera Affiliate, or securely destroy all Idera Personal Data and certify to Idera or, where applicable, an Idera Affiliate that it or they have done so, unless a European Union or European Member State law to which the Partner or a subprocessor are subject prevent the Partner or subprocessor from returning or destroying all or part of the Idera Personal Data. In such a case, the Partner warrants that it will guarantee the confidentiality of Idera Personal Data and will not actively process Idera Personal Data anymore, and will guarantee the return and/or destruction of the Idera Personal Data as requested by Idera when the legal obligation to not return or destroy the information is no longer in effect.

9. **RECORDS AND PROOFS**

- 9.1 Partner warrants it keeps records concerning its security, and organizational technical measures as well as records on any security incident affecting Idera's Personal Data. Such records shall be made available in a standard format immediately exploitable, upon Idera's or, where applicable, an Idera Affiliate's request in the course of a security check or in the framework of an audit.

10. **TERM, PORTABILITY AND REVERSIBILITY AND SURVIVAL**

- 10.1 This DPA is attached to and part of a Partner's agreement executed with Idera or, where applicable, an Idera Affiliate, and shall remain in full force as long as such agreement remains in full force. In order to ensure portability of the Personal Data, and should the agreement be terminated for any reason, Partner shall, within five (5) days of Idera's or, where applicable, an Idera Affiliate's request, make available Idera's Personal Data in a standard format. Such Information shall include account level information including IP addresses, hostnames, infrastructure information and Idera or, where applicable, an Idera Affiliate contact information.
- 10.2 Survival. Any terms of this DPA which by their nature should survive the termination of this DPA shall survive such termination.

11. **MISCELLANEOUS**

- 11.1 In the event of inconsistencies between the provisions of this DPA and other agreements between the parties, the provisions of this DPA shall prevail with regard to the parties' data protection obligations relating to Idera Personal Data. In cases of doubt, this DPA shall prevail, in particular, where it cannot be clearly established whether a clause relates to a party's data protection obligations.
- 11.2 Should any provision or condition of this DPA be held or declared invalid, unlawful or unenforceable by a competent authority or court, then the remainder of this DPA shall remain valid. Such an invalidity, unlawfulness or unenforceability shall have no effect on the other provisions and conditions of this DPA to the maximum extent permitted by law. The provision or condition affected shall be construed either: (a) to be amended in such a way that ensures its validity, lawfulness and enforceability while preserving the parties' intentions, or if that is not possible, (ii) as if the invalid, unlawful or unenforceable part had never been contained in this DPA.
- 11.3 Any amendments to this DPA shall be in writing duly signed by authorised representatives of the parties hereto.

12. **PRIVACY SHIELD**

- 12.1 If at any time after the date of this Agreement, Idera or, where applicable, an Idera Affiliate elects to be certified under the EU-U.S. Privacy Shield and/or the Swiss-U.S. Privacy Shield (collectively, "Privacy Shield"), Partner further agrees: (i) to Process and transfer Personal Information only for the limited and specified purposes under this Agreement; (ii) to provide at least the same level of privacy protection as is required by the principles of

Privacy Shield; (iii) upon reasonable notice, to permit Idera or, where applicable, an Idera Affiliate to perform an audit at its own expense or to take other reasonable and appropriate steps to ensure that Partner effectively Processes the Personal Information transferred under this Agreement in a manner consistent with Partner's obligations under Privacy Shield; (iv) upon notice, to take reasonable and appropriate steps to stop and remediate any unauthorized Processing hereunder; (v) to permit Idera or, where applicable, an Idera Affiliate to provide a summary or a representative copy of the relevant privacy provisions of this Agreement to the U.S. Department of Commerce upon the Department of Commerce's request; and (vi) to notify Idera or, where applicable, an Idera Affiliate if Partner determines it can no longer meet the obligations under this Section.

***[SIGNATURE PAGE FOLLOWS]***

**Data exporter: Idera, Inc., acting on its behalf and on behalf of each Idera Affiliate, as set forth on Exhibit A hereto, pursuant to powers of attorney.**

Name (written out in full):           Trey Chambers  
Position:                                Chief Financial Officer  
Address:                                 10801 North Mopac Expressway  
  Building 1, Suite 100  
  Austin, TX 78759

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

**On behalf of the data importer (Partner/Reseller/Distributor company full legal name): \_\_\_\_\_**

Name (written out in full): \_\_\_\_\_

Position: \_\_\_\_\_

Address: \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

**SCHEDULE 1**  
**Standard Contractual Clauses: C-to-P Transfer**

**1. DEFINITIONS**

For the purposes of the Clauses:

- (a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- (b) *'the data exporter'* means the controller who transfers the personal data;
- (c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- (d) *'the sub-processor'* means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- (e) *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- (f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

**2. DETAILS OF THE TRANSFER**

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 of Schedule 1 which forms an integral part of the Clauses.

**3. THIRD-PARTY BENEFICIARY CLAUSE**

- 3.1 The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6.1 and 6.2, Clause 7, Clause 8.2, and Clauses 9 to 12 as third-party beneficiary.
- 3.2 The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8.2, and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
- 3.3 The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8.2, and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
- 3.4 The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.



#### 4. **OBLIGATIONS OF THE DATA EXPORTER**

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 of Schedule 1;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8.3 to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- (j) that it will ensure compliance with Clause 4(a) to (i).

#### 5. **OBLIGATIONS OF THE DATA IMPORTER**

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the

Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 of Schedule 1 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
  - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
  - (ii) any accidental or unauthorised access, and
  - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 of Schedule 1 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- (h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

## 6. **LIABILITY**

- 6.1 The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.
- 6.2 If a data subject is not able to bring a claim for compensation in accordance with paragraph 6.1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.
- 6.3 If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 6.1 and 6.2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law

or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

**7. MEDIATION AND JURISDICTION**

7.1 The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

- (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
- (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

7.2 The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

**8. COOPERATION WITH SUPERVISORY AUTHORITIES**

8.1 The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

8.2 The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

8.3 The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 8.2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

**9. GOVERNING LAW**

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

**10. VARIATION OF THE CONTRACT**

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clauses.

**11. SUB-PROCESSING**

11.1 The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

11.2 The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in Clause 6.1 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

11.3 The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 11.1 shall be governed by the law of the Member State in which the data exporter is established.

11.4 The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

12. **OBLIGATION AFTER THE TERMINATION OF PERSONAL DATA PROCESSING SERVICES**

12.1 The parties agree that on the termination of the provision of data processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

12.2 The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 12.1.

13. **LIABILITY**

The parties agree that if data exporter is held liable for a violation of the clauses committed by the data importer, the data importer will, to the extent to which it is liable, indemnify the data exporter for any cost, charge, damages, expenses or loss it has incurred. The parties agree that no limitation of liability contained in any other agreement between the parties shall apply to this Clause 13. The Indemnification is contingent upon: (a) the data exporter promptly notifying the data importer of a claim; and (b) the data importer being given the possibility to cooperate with the data exporter in the defence and settlement of the claim.

**[SIGNATURE PAGE FOLLOWS]**

**Data exporter: Idera, Inc. acting on its behalf and on behalf of each Idera Affiliate, as set forth on Exhibit A hereto, pursuant to powers of attorney.**

Name (written out in full):           Trey Chambers  
Position:                                Chief Financial Officer

Address:                                10801 North Mopac Expressway,  
  Building 1, Suite 100  
  Austin, TX 78759

Signature: \_\_\_\_\_  
Date: \_\_\_\_\_

**On behalf of the data importer (Partner/Reseller/Distributor company full legal name): \_\_\_\_\_**

Name (written out in full): \_\_\_\_\_  
Position: \_\_\_\_\_  
Address: \_\_\_\_\_

Signature: \_\_\_\_\_  
Date: \_\_\_\_\_

**APPENDIX 1 OF SCHEDULE 1**  
**DESCRIPTION OF THE TRANSFERS (CONTROLLER TO PROCESSOR)**

**Data exporter**

The Data Exporter is Idera, Inc, acting on its behalf and on behalf of each Idera Affiliate, as set forth on Exhibit A, is a **global provider of software products and services**.

**Data importer**

The Data Importer is the Partner agreeing to these terms. The Data Importer processes Personal Data of data exporter's personnel and/or customers/end-users and/or prospect customers upon the instructions of the data exporter in accordance with the terms of this DPA and the Agreement between the Data Exporter and Data Importer relating to the provisions of services by Data Importer to Idera (and/or any of its affiliates listed in the attached Exhibit A).

**Data subjects**

The personal data transferred concern the following categories of data subjects (please specify):

Data exporter may submit Personal Data, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subject: prospects, customers, business partners and Partners of data exporter (who are natural persons); subscribers/users; employees or contact persons of data exporter's prospects, customers, business partners and Partners; employees, agents, advisors, freelancers of data exporter (who are natural persons).

**Categories of data**

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

Data exporter may submit Personal Data, the extent of which is determined, applicable and controlled by the data exporter in its sole discretion, and which may include, but is not limited to: first and last name; title; position; employer; contact information (including, but not limited to, company, email, phone, and physical business address) ID data (including, but not limited to, employee number), professional life data, connection data, localization data, communication data, and traffic data.

**Special categories of data (if appropriate)**

The personal data transferred concern the following special categories of data (please specify): Not Applicable.

**Processing operations**

The personal data transferred will be subject to the following basic processing activities (please specify): The objective of Processing of Personal Data by data importer is the performance of the data importer's services pursuant to the Agreement between the data exporter and data importer relating to the provision of services by data importer to data exporter.

## Appendix 2 of Schedule 1

### Technical and Organisational Security Measures

**This Appendix 2 forms part of the Transfer Clauses and summarizes the technical, organisational and physical security measures implemented by the parties in accordance with Clauses 4(d) and 5(c).**

In addition to any data security requirements set forth in the Agreement, Partner shall comply with the following:

**I - Physical Access Control:** *Unauthorised persons shall be prevented from gaining physical access to premises, buildings or rooms where personal data processing systems are located.* The processor has implemented the following controls (without limitation):

1. The processor prevents unauthorized individuals from gaining access to the processor's premises.
2. The processor restricts access to data centres / rooms where data servers are located.
3. The processor uses video surveillance and intrusion detection devices to monitor access to data processing facilities.
4. The processor ensures that individuals who do not have access authorization (e.g. technicians, cleaning personnel) are accompanied at all times when accessing data processing facilities.

**II – System Access Control:** *Data processing systems must be prevented from being used without authorization.* The processor has implemented the following controls (without limitation):

1. The processor implements measures to prevent unauthorised personnel from accessing data processing systems.
2. The processor provides dedicated user IDs for every authorised personnel accessing data processing systems for authentication purposes.
3. The processor assigns passwords to all authorised personnel for authentication purposes.
4. The processor ensures that all data processing systems are password protected to prevent unauthorised persons accessing any personal data: (a) after boot sequences; and (b) when left unused for a short period.
5. The processor ensures that access control is supported by an authentication system.
6. The processor has implemented a password policy that prohibits the sharing of passwords, outlines processes after a disclosure of a password, and requires the regular change of passwords.
7. The processor ensures that passwords are always stored in encrypted form.
8. The processor implements a proper procedure to deactivate user accounts when a user leaves the processor (or processor function).
9. The processor implements a proper process to adjust administrator permissions when an administrator leaves the processor (or processor function).

**III – Data Access Control:** *Persons entitled to use a data processing system shall gain access only to the data to which they have a right of access, and personal data must not be read, copied, modified or removed without authorization in the course of processing or use and after storage.* The processor has implemented the following controls (without limitation):

1. The processor ensures that personal data cannot be read, copied, modified or removed without authorization during processing or use and after storage.
2. The processor grants data access only to authorized personnel and assigns only the minimum data permissions necessary for those personnel to fulfil their duties.
3. The processor ensures that the personnel who use the data processing systems can access only the data to which they have a right of access.
4. The processor restricts access to files and programs based on a "need-to-know-basis".
5. The processor stores physical media containing personal data in secured areas.
6. The processor has measures in place to prevent use/installation of unauthorised hardware and/or software.
7. The processor has established rules for the safe and permanent destruction of data that are no longer required.

**Data exporter: Idera, Inc. acting on its behalf and on behalf of each Idera Affiliate, as set forth on Exhibit A hereto, pursuant to powers of attorney.**

Name (written out in full):                   Trey Chambers  
Position:                                        Chief Financial Officer

Address:                                        10801 North Mopac Expressway,  
  Building 1, Suite 100  
  Austin, TX 78759

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

**On behalf of the data importer (Partner/Reseller/Distributor company full legal name): \_\_\_\_\_**

Name (written out in full): \_\_\_\_\_

Position: \_\_\_\_\_

Address: \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_\_



**Exhibit A**  
**List of Idera, Inc. group companies**

Idera hereby represents and warrants that each of the following entities is a an Idera Affiliate (as defined in the Data Processing Agreement for Resellers, Distributors and Partners to which this Exhibit A is attached (the “DPA”) and that Idera has the valid power to bind each of the Idera Affiliate to the DPA. This Exhibit A may be amended unilaterally by Idera, from time to time, in order to add entities that subsequently become or qualify as an Idera Affiliate and upon such amendment, such additional entities shall be deemed an Idera Affiliate under and party to the DPA. In addition, Idera may assign this DPA to an affiliated company or as part of a corporate reorganization, consolidation, merger, or sale of all or substantially all of the assets to which this DPA relates.

TA Buckeye Parent LLC	c/o TA Associates Management LP 200 Clarendon Street, 56th Floor Boston, MA 02116
TA Buckeye Intermediate Corporation	c/o TA Associates Management LP 200 Clarendon Street, 56th Floor Boston, MA 02116
Idera, Inc.	2950 North Loop West Brookhollow III, Suite 700 Houston, Texas 77092
Shiner Acquisition First Corp.	2950 North Loop West Brookhollow III, Suite 700 Houston, Texas 77092
Precise Software Solutions, Inc.	2950 North Loop West Brookhollow III, Suite 700 Houston, Texas 77092
Uptime Software, Inc.	2950 North Loop West Brookhollow III, Suite 700 Houston, Texas 77092
Precise Software Solutions UK Limited	York House 18 York Road Maidenhead, Berkshire SL6 1SF United Kingdom
EMBT Holdings Inc.	10801 N Mopac Expressway Building 1, Suite 100 Austin, Texas 78759
EMB Holding Corp.	10801 N Mopac Expressway Building 1, Suite 100 Austin, Texas 78759
Embarcadero Technologies, Inc.	10801 N Mopac Expressway Building 1, Suite 100 Austin, Texas 78759
CodeGear LLC	10801 N Mopac Expressway Building 1, Suite 100 Austin, Texas 78759
Embarcadero Technologies Europe Ltd. - France Representative Office	York House 18 York Road Maidenhead, Berkshire

- Moscow Representative Office	SL6 1SF United Kingdom
Embarcadero Germany GmbH	Südliche Ringstraße 175 Langen, 63225 Germany
Embarcadero Technologies Singapore Pte. Ltd.	3 Raffles Place #07-01 Bharat Building Singapore, 048617
Embarcadero Technologies GK	Sumitomo Fudosan Idabashi Building 2-3-21 Koraku, Bunkyo-ku Tokyo 112-0004 Japan
Embarcadero Technologies India Private Limited	Level 2 Wing A DivyaSree Chambers 11 O'Shaughnessy Road Langford Town Bangalore, 560025 India
Gurock Software GmbH	Südliche Ringstraße 175 Langen, 63225 Germany
AquaFold, Inc.	10801 N Mopac Expressway Building 1, Suite 100 Austin, Texas 78759
Sencha, Inc.	10801 N Mopac Expressway Building 1, Suite 100 Austin, Texas 78759
Ranorex GmbH	Strassganger Strasse 289 8053 Graz Austria
Ranorex Inc.	10801 N Mopac Expressway Building 1, Suite 100 Austin, Texas 78759
Webyog, Inc.	10801 N Mopac Expressway Building 1, Suite 100 Austin, Texas 78759
Webyog Softworks Private Limited	SVR Complex, 1st Floor, Hosur Road Madiwala, Bangalore 560 068 India
Froala Labs SA	19-21 Bucuresti - Ploiesti Avenue 6th floor, office no. R.4 1st District, Bucharest Bucharest, Romania 19-21 Bucuresti - Ploiesti Avenue
Whole Tomato Software, LLC	10801 N Mopac Expressway Building 1, Suite 100 Austin, Texas 78759

Kiuwan Software, S.L.	Calle Norias, no.80 PC 28221 Majadahonda, Madrid, Spain
Assembla, Inc.	10801 N Mopac Expressway Building 1, Suite 100 Austin, Texas 78759
Assembla Europe Ltd. (Formally: Cogneto Software Consulting)	Unit 1, CHQ Building Custom House Quay Dublin 1, Ireland
LANSA Holdings, Inc.	10801 N Mopac Expressway Building 1, Suite 100 Austin, Texas 78759
LANSA, Inc. - Canada Branch Office	2001 Butterfield Road Suite 102 Downers Grove, Illinois 60515
LANSA, Ltd. - France Branch Office - Netherlands Branch Office	23-3 Upper Marlborough Road St. Albans Hertfordshire ALI 3UU, England
LANSA Pty, Ltd. - Singapore Branch Office	122 Arthur Street, North Sydney Australia NSW 2060
LANSA Philippines, Inc.	Unit 2003, 20 <sup>th</sup> Floor, Philippines Aza Life Center Gil Puvat Avenue Makati City, Philippines
LANSA Japan, Ltd.	BC Plaza, 5 <sup>th</sup> Floor, 2-3-20 Kudanminami, Chjiyoda-ku Tokyo Japan 102-0074
Travis CI GmbH	Rigaer Str. 8 10247 Berlin, Germany
Travis CI UG	Rigaer Str. 8 10247 Berlin, Germany
Travis CI Corporation	10801 N Mopac Expressway Building 1, Suite 100 Austin, Texas 78759
WhereScape, Inc.	10801 N Mopac Expressway Building 1, Suite 100 Austin, Texas 78759
WhereScape Europe Limited	450 Brook Drive Green Park Reading United Kingdom RG2 6UU
FusionCharts, Inc.	10801 N Mopac Expressway Building 1, Suite 100 Austin, Texas 78759
Qubole, Inc.	10801 N Mopac Expressway Building 1, Suite 100 Austin, Texas 78759

Qubole Software India Pvt. Ltd.	BDA Site No. 256, HSR LAYOUT 6th Sector 17th Cross 5th Main Bengaluru Karnataka 560102 India
Qubole Ltd.	Eastbourne Terrace London W2 6LG
Qubole, Pte. Ltd	10801 N Mopac Expressway Building 1, Suite 100 Austin, Texas 78759
apilayer Data Products GmbH	EllisabethstraBe 15/5A +5B 1010 Viena