Jurisdiction Specific Terms
(Customer-Facing DPA)

These Jurisdiction Specific Terms are an integral part of the Data Processing Agreement ("**DPA**") entered into between the entity identified as "**Customer**" and Idera, Inc. or any of Idera Affiliates (collectively, "**Idera**").

Capitalized terms which are used but not defined in this document shall have the meaning given to those terms in the DPA. By signing the DPA, the Parties have agreed to comply with these Jurisdiction Specific Terms which apply to the extent that the Parties Process Customer PersonalData originating from, or protected by, Applicable Data Protection Laws in one of the jurisdictions identified herein.

1. European Economic Area and Switzerland.

1.1. Definitions:

(a) For the purpose of interpreting the DPA, the following terms shall have the meanings setout below:

i. "**Applicable Data Protection Laws**" (as used in the DPA) includes the (i) EEA Data Protection Laws and (ii) Swiss Data Protection Laws.

ii. "**Controller"** includes "**Controller of the Data File**" as defined under the FADP (as defined below).

iii. "**Data Subject**" includes the natural persons whose Personal Data is Processed.

iv. "**EEA**" means the European Economic Area, consisting of the EU Member States, and Iceland, Liechtenstein, and Norway.

v. "**EEA Data Protection Laws**" means the EU Data Protection Directive 95/46/EC and implementing legislation, the EU GDPR and the laws implementing or supplementing the EU GDPR;

vi. "**EU 2021 Standard Contractual Clauses**" means the contractual clauses adopted by the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

vii. "**EEA Restricted Transfer**" includes any transfer of Personal Data subject to EEA Data Protection Laws (including data storage on foreign servers) which is undergoing Processing or is intended for Processing after transfer, to a Third Country (as defined below) or to an international organization.

viii. "**Personal Data**" includes "**Personal Data**" as defined under the FADP.

ix. "**Processing**" includes "**Processing**" as defined under the FADP.

x. "**Standard Contractual Clauses**" (as defined in the DPA) includes the EU 2021 Standard Contractual Clauses.

xi. "**Swiss Data Protection Laws**" includes the Swiss Federal Act on Data

Protection of 19 June 1992 ("**FADP**") and the Ordinance to the Federal Act on Data Protection ("**OFADP**"), as they may be amended from time to time.

xii. "**Restricted Transfer of Swiss Data**" includes any transfer of Personal Data (including data storage in foreign servers) subject to the FADP to a Third Country or an international organization.

xiii. "**Third Country**" (as used in this Section) means a country outside of the EEA.

1.2. Transfer Mechanisms:

(a) With regard to any EEA Restricted Transfer or Restricted Transfer of Swiss Data from Customer to Idera within the scope of the DPA, one of the following transfer mechanisms shall apply, in the following order of precedence:

i. a valid adequacy decision pursuant to the requirements under the EU GDPR that provides that the third country or the international organization in question to which Customer Personal Data is to be transferred ensures an adequate level of data protection or the inclusion of such third country or international organization in the list published by the Swiss Federal Data Protection and Information Commissioner of states that provide an adequate level of protection for Personal Data within the meaning of Swiss Data Protection laws;

ii. Idera's certification to any successor to the Privacy Shield Framework (only to theextent that such self-certification constitutes an "appropriate safeguard" pursuant to the EU GDPR, as the case may be), provided that the Services are covered by the self-certification;

iii. the EU 2021 Standard Contractual Clauses (insofar as their use constitutes an "appropriate safeguard" under EEA Data Protection Laws or Swiss Data Protection Laws, as the case may be); or

iv. any other lawful basis, as laid down in EEA Data Protection Laws or Swiss Data Protection Laws, as the case may be.

1.3. EU 2021 Standard Contractual Clauses:

(a) The DPA hereby incorporates by reference the EU 2021 Standard Contractual Clauses. The Parties are deemed to have accepted, executed, and signed the Standard Contractual Clauses where necessary in their entirety (including the annexures thereto).

(b) The content of EU 2021 Annex I and Annex II of the EU 2021 Standard Contractual Clauses is set forth in the Idera Affiliates Data Processing Terms.

(c) The text contained in **Annex A** to these Jurisdiction Specific Terms supplements the EU 2021 Standard Contractual Clauses.

(d) The Parties agree to apply the following modules:

i. Module two of the EU 2021 Standard Contractual Clauses when, in accordance with Section 2(a) of the DPA, the Data Exporter is Customer and acts as a

Controller and the Data Importer is Idera and acts as a Processor; and

ii. Module three of the EU 2021 Standard Contractual Clauses when, in accordance with Section 2(a) of the DPA, the Data Exporter is Customer and acts as a Processor and the Data Importer is Idera and acts as a sub-Processor.

iii. Module four of the EU 2021 Standard Contractual Clauses when, in accordance with Section 2(a) of the DPA, the Data Exporter is Idera and acts as a Processor and Data Importer is Customer and acts as Controller.

(e) For the purposes of Annex I.A:

i. The Parties have provided each other with the identity information contact details required under Annex I.A.

ii. The Parties' controllership roles are set forth in Section 3.1 of the DPA.

iii. The details of Idera's data protection officer and data protection representative in the EU are set forth in the Idera Affiliate Processing Terms and Section 9 of the DPA.

iv. The activities relevant to the Customer Personal Data transferred under the EU 2021 Standard Contractual Clauses are set forth in the Idera Affiliate Processing Terms.

(f) Parties' Choices under the EU 2021 Standard Contractual Clauses:

i. For the purposes of Clause 7 of the EU 2021 Standard Contractual Clauses, the Parties choose not to include the optional docking clause.

ii. With respect to Clause 9 of the EU 2021 Standard Contractual Clauses, the Parties select the "Option 2 General Written Authorization" and the time period set forth in Section 2(e) of the DPA.

iii. For the purpose of Clause 11 of the EU 2021 Standard Contractual Clauses, the Parties choose not to include the optional language relating to the use of an independent dispute resolution body.

iv. For the purpose of Annex I.C and with respect to Clause 13 (when applicable) of the EU 2021 Standard Contractual Clauses: If Customer, the data exporter, is established in an EU Member State, it elects the supervisory authority of the jurisdiction where it established as the competent supervisory authority responsible for ensuring compliance by the data exporter with the EU GDPR as regards to the data transfer. If Customer, the data exporter, is not established in an EU Member State, but falls within the territorial scope of application of Article 3(2) of the EU GDPR and it has appointed a representative established in a EU Member State, the supervisory authority of the jurisdiction where the representative is established shall act as the competent supervisory authority and be responsible for ensuring compliance by the data exporter with the EU GDPR as regards to the data transfer. If the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Article 3(2) of the EU GDPR and it has not

appointed a representative according to Art. 27 EU GDPR, the competent supervisory authority shall be the Ireland Data Protection Commission. To the extent the data transfer constitutes a Restricted Transfer of Swiss Data, the competent authority shall be the Swiss Federal Data protection and Information Commissioner.

v. With respect to Clause 17 of the EU 2021 Standard Contractual Clauses, the Parties select the law of the Republic of Ireland.

vi. With respect to Clause 18 of the EU 2021 Standard Contractual Clauses, the Parties agree that any dispute arising from the EU 2021 Standard Contractual Clauses shall be resolved by the courts of the Republic of Ireland. The Parties choose the Swiss courts as an alternative place of jurisdiction for data subjects habitually resident in Switzerland.

(g) The term "**member state**" included in the EU 2021 Standard Contractual Clauses must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EU 2021 Standard Contractual Clauses.

(h) With respect to Restricted Transfers of Swiss Personal Data, the Parties acknowledge that the EU 2021 Standard Contractual Clauses also protect the data of legal entities until the entry into force of the revised FADP.

1.2. In cases where the EU 2021 Standard Contractual Clauses apply and there is a conflict between the terms of the DPA and the terms of the EU 2021 Standard Contractual Clauses, the terms of the EU 2021 Standard Contractual Clauses shall prevail.

1.3. Agreements with Subprocessors

(a) Idera shall ensure that the arrangement between Idera and any Subprocessor is governed by a written contract that includes data protection obligations compatible with those of Idera under the DPA and this Section. Customer agrees that older versions of the Standard Contractual Clauses concluded between Idera and Subprocessor provide for the same level of protection for Customer Personal Data as those set out in the DPA between Customer and Idera.

2. California

2.1. Definitions:

(a) For the purpose of interpreting the DPA, the following terms shall have the meanings setout below:

i. "**Applicable Data Protection Laws**" includes California Data Protection Laws, as may be amended from time to time.

ii. "**California Data Protection Laws**" includes the CCPA and the CCPA Regulations.

iii. "**CCPA**" means the California Consumer Privacy Act of 2018;

iv. "**CCPA Regulations**" means the California Consumer Privacy Act Regulations;

(b) The terms "**Business Purpose**", "**Commercial Purpose**", "**Sale**", "**Sell**", along with

their cognates whether capitalized or not, shall have the same meaning as in the CCPA, and their related terms shall be construed accordingly.

(c) For the purpose of interpreting the DPA, the following terms shall be interpreted as follows:

i. "**Controller**" includes "**Business**" as defined under the CCPA;

ii. "**Data Subject**" includes "**Consumer**" as defined under the CCPA;

iii. "**Personal Data**" includes "**Personal Information**" as defined under the CCPA;

iv. "**Personal Data Breach**" includes "**Breach of the Security of the System**" as defined in Section 1798.8 of the California Civil Code;

v. "**Processor**" includes "**Service Provider**" as defined under the CCPA;

2.2. Idera as a Service Provider:

(a) Where Idera acts as a Data Processor or a sub-Processor on behalf of Customer in accordance with Section 2(a) of the DPA:

i. Customer discloses Customer Personal Data to Idera solely for: (i) valid Business Purposes; and (ii) to enable Idera to perform the Processor Services under the Main Agreement(s).

ii. Idera shall not: (i) sell Personal Data; or (ii) retain, use or disclose Customer PersonalData for any purpose other than providing the Processor Services specified in the Main Agreement(s) or as otherwise permitted by the CCPA and the CCPA Regulations. Idera certifies that it understands these restrictions and will comply with them.

3. Canada

3.1. Definitions:

(a) For the purpose of interpreting the DPA, the following terms shall have the meanings setout below:

i. "**Applicable Data Protection Laws**" includes PIPEDA (as defined below).

ii. "**Personal Data**" includes "**Personal Information**" as defined under PIPEDA (asdefined below).

iii. "**Personal Data Breach**" includes "**Breach of Security Safeguards**" as defined under PIPEDA (as defined below).

iv. "**PIPEDA**" means the Federal Personal Information Protection and Electronic Documents Act.

v. **"Sub-Processor**" includes "**Third Party Organization**" as defined under PIPEDA.

3.2. **Necessary Consent.** Customer confirms that it has obtained valid consent (as defined under PIPEDA), where necessary to Process Personal Data of each Data Subject.

4. United Kingdom

4.1. Definitions:

(a) For the purpose of interpreting the DPA, the following terms shall have the meaningsset out below:

i. "**Applicable Data Protection Laws**" (as used in the DPA) includes UK Data Protection Laws (as defined below).

ii. "**EU 2021 Standard Contractual Clauses**" (as used in this Section) means the contractual clauses adopted by the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

iii. "**Restricted Transfer of UK Data**" (as used in this Section) includes any transfer of Personal Data subject to UK Data Protection Laws to a Third Country or an international organization (including data storage on foreign servers).

iv. "**Standard Contractual Clauses**" (as used in the DPA) includes the EU 2021 Standard Contractual Clauses (as defined under Section 1.1(a)vi of these Jurisdiction Specific Terms).

v. "**Third Country**" (as used in this Section) means a country outside of the United Kingdom ("**UK**").

vi. "**UK Data Protection Laws**" (as used in this Section) includes the UK GDPR (as defined below) and the UK Data Protection Act 2018.

vii. "**UK GDPR**" (as used in this Section) means the UK General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

viii. "**UK ICO**" (as used in this Section) means the UK Information Commissioner's Office.

ix. "**UK International Data Transfer Agreement**" (as used in this Section) means the International Data Transfer Agreement issued by the UK ICO, Version A1.0, in force from 21 March 2022, as may be amended from time to time, available at ICO website at https://ico.org.uk/media/for-organisations/documents/4019538/international-data-transfer-agreement.pdf.

x. "**UK Transfer Addendum**" (as used in this Section) means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK ICO, Version B1.0, in force from 21 March 2022, as may be amended from time to time, available at ICO website at https://ico.org.uk/media/for-organisations/documents/4019483/international-data-transfer-addendum.pdf.

4.2. Restricted Transfers of UK Data:

(a) With regard to any Restricted Transfer of UK Data from Customer to Idera within the scope of the DPA, one of the following transfer mechanisms shall apply, in the following order of precedence:

i. a valid adequacy decision pursuant to Article 45 of the UK GDPR that provides

that the Third Country, a territory or one or more specified sectors within that Third Country, or the international organization in question to which Personal Data is to be transferred ensures an adequate level of data protection;

ii. Service Provider's self-certifications to any successor or replacement framework to the EU-U.S. Privacy Shield Framework (only to the extent that such a framework has been granted an adequacy decision by the UK Data Protection Laws, as the case may be), provided that the Services are covered by such certification;

iii. the EU 2021 Standard Contractual Clauses (as defined under Section 1.1(a)vi of these Jurisdiction Specific Terms) (insofar as their use constitutes an "appropriate safeguard" under the UK Data Protection Laws, and to the extent that the Data Importer is not directly subject to the UK GDPR on an extra-territorial basis) as they have been adopted for use by the relevant authorities within the UK, including the UK ICO, using the UK Transfer Addendum;

iv. the UK International Data Transfer Agreement;

v. any other lawful basis, as laid down in the UK Data Protection Laws, as the case may be.

4.3. EU 2021 Standard Contractual Clauses and UK Transfer Addendum:

(a) The DPA hereby incorporates by reference any additional modifications and amendments required by the UK Transfer Addendum as they have been adapted for use by the relevant authorities within the UK to make the EU 2021 Standard Contractual Clauses applicable to Restricted Transfers of UK Data. The Parties are deemed to have accepted, executed, and signed the adapted EU 2021 Standard Contractual Clauses where necessary in their entirety (including the annexures and any addenda thereto).

(b) For the purposes of the tables to the UK Transfer Addendum:

i. Table 1: The content of Table 1 is set forth in Section 9 of the DPA.

ii. Table 2: The content of Table 2 is set out in Section (c) of these Jurisdiction Specific Terms. The Parties agree that Modules two, three, and four of the EU 2021 Standard Contractual Clauses are applicable. To the extent that Module four is applicable, the Parties confirm that Personal Data received from the Data Importer [is][is not] combined with personal data collected by the Data Exporter.

iii. Table 3: The applicable content of Table 3 (Annex 1(A), 1(B), II, and III) is set forth as follows:

(A) *Annex 1(A)*: The content of Annex 1(A) is set forth in Section 9 of the DPA and **Appendix 1** thereto.

(B) *Annex 1(B)*: The content of Annex 1(B) is set forth in Section 2(d) of the DPA and **Appendix 1** thereto.

(C) *Annex II*: The content of Annex II is set forth in Section 3 of the DPA and **Appendix 1** thereto.

(D) *Annex III*: This is not required, as "General Written Authorization" has been selected under the EU 2021 Standard Contractual Clauses.

iv. Table 4: The Parties agree that neither Party may terminate the UK Transfer Addendum.

(c) Beyond that, the Parties incorporate and adopt the EU 2021 Standard Contractual Clauses as to Restricted International Transfers of UK Personal Data in exactly the same manner set forth in Section 1.3 of these Jurisdiction Specific Terms, with the following distinctions:

i. For the purpose of Annex I.C and with respect to Clause 13 (when applicable) of the EU 2021 Standard Contractual Clauses, the competent authority shall be the UK ICO, insofar as the data transfer constitutes a Restricted Transfer of UK Data.

ii. With respect to Clause 17 of the EU 2021 Standard Contractual Clauses, including the incorporated UK Transfer Addendum, the Parties select the laws of England and Wales.

iii. With respect to Clause 18 of the EU 2021 Standard Contractual Clauses, including the incorporated UK Transfer Addendum, the Parties agree that any dispute arising from the EU 2021 Standard Contractual Clauses or the incorporated UK Transfer Addendum shall be resolved by the courts of England and Wales. A Data Subject may also bring legal proceedings against the Data Exporter and/or Data Importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.

(d) The text contained in **Annex A** to these Jurisdiction Specific Terms supplements the EU 2021 Standard Contractual Clauses.

(e) In cases where the EU 2021 Standard Contractual Clauses, in conjunction with the UK Transfer Addendum, apply and there is a conflict between the terms of the DPA and the terms of the EU 2021 Standard Contractual Clauses or UK Transfer Addendum, the terms of the UK Transfer Addendum, and then the EU 2021 Standard Contractual Clauses, shall prevail.

4.4. UK International Data Transfer Agreement:

(a) The DPA hereby incorporates by reference the UK International Data Transfer Agreement. The Parties are deemed to have accepted, executed, and signed the UK International Data Transfer Agreement where necessary in its entirety.

(b) For the purposes of the tables to the UK International Transfer Agreement:

i. Table 1: The content of Table 1 is set forth in Section 9 of the DPA and **Appendix 1** thereto.

ii. Table 2:

(A) The UK International Transfer Agreement shall be governed by the laws of England and Wales.

(B) The Parties agree that any dispute arising from the UK International Transfer Agreement shall be resolved by the courts of England and Wales.

(C) The Parties' controllership and data transfer roles are set out in Section 2(a) of the DPA.

(D) The UK GDPR applies to the Data Importer's Processing of the Personal Data.
(E) These Jurisdiction Specific Terms and the DPA set out the instructions for Processing Personal Data.
(F) The Data Importer shall Process Personal Data for the time period set out in **Appendix 1** of the DPA. The Parties agree that neither Party may terminate the UK International Transfer Agreement before the end of such time period.
(G) The Data Importer may only transfer Personal Data to authorized Subprocessors (if applicable), as set out in Section 2(e) of the DPA, or to such third parties that the Data Exporter authorizes in writing or within the Agreement.
(H) Each Party must review the DPA (including **Appendix 1** and these Jurisdiction Specific Terms) at regular intervals, to ensure that the DPA remains accurate and up to date and continues to provide appropriate safeguards to the Personal Data. Each Party will carry out these reviews as frequently as at least once each year or sooner.

iii. Table 3: The content of Table 3 is set forth in **Appendix 1** of the DPA and may be updated in accordance with Section 2(d) of the DPA.

iv. Table 4: The content of Table 4 is set forth in **Appendix 1** of the DPA and may be updated in accordance with Section 2(d) of the DPA.

(c) Part 2 (Extra Protection Clauses) and Part 3 (Commercial Clauses) of the UK International Transfer Agreement are noted throughout the DPA.

(d) The text contained in **Annex A** to these Jurisdiction Specific Terms supplements the UK International Transfer Agreement.

(e) In cases where the UK International Transfer Agreement applies and there is a conflict between the terms of the DPA and the terms of the UK International Transfer Agreement, the terms of the UK International Transfer Agreement shall prevail.

Annex A to Jurisdiction Specific

Terms Supplemental Clauses to the Standard Contractual

Clauses

By this **Annex A** (this "**Annex**"), the Parties provide additional safeguards and redress to the Data Subjects whose Personal Data is transferred to Idera pursuant to Standard Contractual Clauses. This Annex supplements and is made part of, but is not in variation or modification of, the Standard Contractual Clauses that may be applicable to the Restricted Transfer.

1. Applicability of this Annex

1.1. This Annex only applies with respect to Restricted Transfers when the Standard Contractual Clauses apply to such Restricted Transfers pursuant to the DPA and its Annexes and Idera is the data importer.

2. Definitions

2.1. For the purpose of interpreting this Annex, the following terms shall have the meanings set out below:

(a) "**Disclosure Request**" means any request from law enforcement authority or other governmental authority with competent authority and jurisdiction over Idera for disclosure of transferred Customer Personal Data.

(b) "**EO 12333**" means the U.S. Executive Order 12333.

(c) "**FISA**" means the U.S. Foreign Intelligence Surveillance Act.

(d) "**Schrems II Judgment**" means the judgment of the European Court of Justice in Case C- 311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems.

3. Applicability of Surveillance Laws to Idera

3.1. U.S surveillance laws

(a) Idera represents and warrants that, as of the Effective Date, it has not received any national security orders of the type described in Paragraphs 150-202 of the Schrems II judgment.

(b) Idera represents that it reasonably believes that it is not eligible to be required to provide information, facilities, or assistance of any type under FISA Section 702 because:

i. Idera is not: (i) a telecommunications carrier, (ii) a provider of electronic communication service; (iii) a provider of processing services by means of an electronic communications system to the general public, given the nature of its business-to-business services; or (iv) any other communication service provider whohas access to wire or electronic communications either as such communications are transmitted or as such communications are stored; nor any other type of "electronic communications service provider" within the meaning of 50 U.S.C. § 1881(b)(4).

ii. If Idera were to be found eligible for process under FISA Section 702, which it believes it is not, it is nevertheless also not the type of provider that is eligible to be subject to UPSTREAM collection pursuant to FISA Section 702, as

described in paragraphs 62 and 179 of the Schrems II judgment.

(c) EO 12333 does not provide the U.S. government the ability to order or demand that Idera provide assistance for the bulk collection of information and Idera shall take no action pursuant to U.S. Executive Order 12333.

3.2. General provisions about surveillance laws applicable to Idera:

(a) Data Importer has no reason to believe that the laws and practices in the third countryof destination of Customer Personal Data applicable to the Processing of CustomerPersonal Data by Idera, including any requests to disclose personal data or measures authorizing access by public authorities, prevent Idera from fulfilling its obligations under the Standard Contractual Clauses (where applicable).

(b) Data Importer commits to provide upon reasonable request information about the laws and regulations in the destination countries of the transferred Customer Personal Data applicable to Data Importer that would permit access by public authorities to the transferred Customer Personal Data, in particular in the areas of intelligence, law enforcement, administrative and regulatory supervision applicable to the transferred data. The Data Importer providing the information referred to in this subparagraph 4 may choose the means to provide the information. Data Exporter agrees to cover the costs associated with any required research.

4. Obligations on Idera Related to Disclosure Requests

4.1. In the event Idera receives a Disclosure Request, Idera shall:

(a) Promptly (and, when possible, before disclosing the Customer Personal Data to the public authority) notify Customer of the Disclosure Request, and, where possible, the Data Subject, unless prohibited by law, or, if so prohibited from notifying Customer, use all lawful efforts to obtain the right to waive the prohibition to communicate information relating to the Disclosure Request to Customer as soon as possible. This includes, but is not limited to, informing the requesting public authority of the incompatibility of the Disclosure Request with the safeguards contained in Standard Contractual Clauses and the resulting conflict of obligations for Idera and documenting this communication.

(b) Ask the public authority that issued the Disclosure Request to redirect its request to the Customer to control conduct of the disclosure.

(c) Not disclose the requested Customer Personal Data until required to do so under theapplicable procedural rules.

(d) Provide the minimum amount of information permissible when responding to the request, based on a reasonable interpretation of the request.

(e) Document all the steps taken by Idera related to the Disclosure Request.

4.2. For the purposes of this Section, lawful efforts do not include actions that would result in civil or criminal penalty such as contempt of court under the laws of the relevant jurisdiction.

5. Information on Requests for Personal Data by Public Authorities

5.1. Where allowed by law, Idera commits to provide Customer with information on all requests for Personal Data by US public authorities which Idera has received over the last five (5) years (if any), in particular in the areas of intelligence, law enforcement, administrative, and regulatory supervision applicable to the transferred data and

comprising information about the requests received, the data requested, the requesting body, and the legal basis for disclosure and to what extent Idera has disclosed the requested Personal Data. Idera may choose the means to provide this information.

6. Backdoors

6.1. Idera certifies that:

(a) It has not purposefully created backdoors or similar programming for governmental agencies that could be used to access Idera's Systems or Customer Personal Data subjectto the Standard Contractual Clauses.

(b) It has not purposefully created or changed its business processes in a manner that facilitates governmental access to Customer Personal Data or systems.

(c) National law or government policy does not require Idera to create or maintain back doors or to facilitate access to Customer Personal Data or systems.

6.2. Customer will be entitled to terminate the contract on short notice in cases in which Idera does not reveal the existence of a back door or similar programming or manipulated business processes or any requirement to implement any of these or fails to promptly inform Customer once their existence comes to its knowledge.

7. Information About Legal Prohibitions

7.1. Where allowed by law, Idera will provide Customer information about the legal prohibitions on Idera to provide information under this Annex. Idera may choose the means to provide this information.

8. Termination

8.1. This Annex shall automatically terminate with respect to the Processing of Customer Personal Data transferred in reliance of the Standard Contractual Clauses if the European Commission or a competent regulator approves a different transfer mechanism that would be applicable to the Restricted Transfers covered by the Standard Contractual Clauses (and if such mechanism applies only to some of the data transfers, this Annex will terminateonly with respect to those transfers) and that does not require the additional safeguards set forth in this Annex.