Customer Data Processing Addendum

This Data Processing Addendum ("Addendum" or "Customer DPA") is part of the agreement between Customer (or "Data Controller") and Deltek, Inc. and/or a Deltek entity that has entered into such agreement ("Deltek" or "Data Processor"), including other applicable and associated written or electronic agreements such as terms of service and terms of use for the purchase of software and services ("Agreement"). This Addendum applies exclusively to the processing of Personal Data of data subjects who are located in the European Economic Area (EEA) or Switzerland. This Addendum reflects agreement regarding the Processing of Personal Data (as defined in the General Data Protection Regulation (EU) 2016/679 (GDPR)), in accordance with the GDPR and any other privacy, data protection or security laws applicable to Personal Data ("Privacy Laws"). This Addendum shall not replace any additional rights relating to Processing of Personal Data previously negotiated by Customer in the Agreement.

In the event of inconsistencies between the provisions of this Addendum and the Agreement, the provisions of this Addendum shall prevail with regard to the parties' data protection obligations for Personal Data of data subjects who are located in the EEA or Switzerland. In the event of any inconsistencies between this Addendum and the Standard Contractual Clauses (SCCs) found in Schedule 1, the SCCs shall prevail.

Capitalized terms not defined within this Addendum shall have meaning set forth in the Agreement or as defined by applicable law, including the GDPR. If not defined in either the Addendum, applicable law or the Agreement, the term shall be given its commonly understood meaning.

In addition to Deltek EU entities and entities located in countries deemed to offer an adequate level of data protection, Personal Data may be processed by Deltek entities outside of the EU and third party subprocessors (pursuant to section 2.12 through 2.14 below). Customer and the Deltek entities outside of the EU that will process Personal Data for purposes of fulfilling the Agreement, including Deltek, Inc., Deltek Australia PTY LTD., WorkBook APAC Ltd., and Deltek Systems (Philippines), Ltd., will execute the SCCs found in Schedule 1 to validate the cross-border transfer of Personal Data from the EEA and/or Switzerland to outside the EEA and Switzerland, 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 and (ii) not covered by a suitable framework recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data.

For the avoidance of doubt, Customer is Data Controller and Deltek and its affiliated entities are Data Processors.

1. Data Controller Responsibilities

1.1 Data Controller will determine the scope, purposes, and manner by which its Personal Data may be Processed by Data Processor. Data Controller's instructions for the Processing of Personal Data shall comply with Privacy Laws.

1.2 Data Controller warrants that it has all necessary rights to provide Personal Data to Data Processor for the Processing to be performed in relation to the Agreement. To the extent required by applicable law, Data Controller is responsible for ensuring that any necessary consents to this Processing are obtained, and for ensuring that a record of such consents is maintained. Data Controller shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Data Controller acquired Personal Data.

2. Data Processor Responsibilities

2.1 **Compliance with Data Controller's instructions for Processing**. Data Processor will Process Personal Data in accordance with the written instructions of Data Controller and any GDPR requirements directly applicable to Data Processor’s provision of services under the Agreement. Data Processor will inform Data Controller if it believes that an instruction by Data Controller violates Privacy Laws.

2.2 **Audits and information necessary to demonstrate compliance.** Data Processor shall make available to Data Controller information necessary to demonstrate compliance with the obligations laid down in this Addendum and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by Data Controller upon Data Controller’s reasonable written request. Unless required by applicable law, the parties agree that any audits will be conducted no more than once in any twelve month period.

2.3 **Assistance with Data Controller obligations**. Data Processor shall provide reasonable assistance to enable Data Controller to comply with its obligations under Articles 32-36 of the GDPR (inclusive) (security of Processing, Personal Data Breach notification, Data Protection Impact Assessments, and prior consultation).

2.4 Subject to the confidentiality obligations set forth in the Agreement, Data Processor will either provide Data Controller the applicable annual SOC 2 Type II Report covering the trust principles of Security, Availability, and Confidentiality, prepared by a reputable independent third-party that attests to the compliance of the applicable security controls with industry standards; or complete a security questionnaire submitted to Data Processor by Data Controller.

2.5 **Maintain records of processing**. Data Processor shall keep records of all Processing of Data Controller’s Personal Data by Data Processor pursuant to Article 30 of the GDPR.

2.6 **Data Processor personnel and confidentiality.** Without prejudice to any existing contractual arrangements between the parties, Data Processor shall treat all Personal Data as strictly confidential and it shall inform its employees, agents, and/or subprocessors engaged in Processing the Personal Data of the confidential nature of the Personal Data and ensure that all relevant employees, agents, and/or subprocessors are committed to a duty of confidentiality.

2.7 **Technical and organizational measures.** 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, without prejudice to any other security standards agreed upon by the parties, Data Controller and Data Processor shall implement appropriate technical and organisational measures to ensure a level of security of the Processing of Personal Data appropriate to the risk.

2.8 **Personal Data Breach notification.** If Data Processor becomes aware of a Personal Data Breach that impacts the Processing of the Personal Data that is the subject of the Agreement, it shall notify Data Controller without undue delay. Data Processor shall reasonably cooperate with Data Controller regarding such Personal Data Breaches. Data Processor endeavours to notify Data Controller of such Personal Data Breaches in no more than 72 hours after discovery.

2.9 **Termination and return/destruction of Personal Data**. Upon Data Controller’s termination of the Agreement, Data Processor shall, at the discretion of Data Controller, either delete, destroy, or return all Personal Data to Data Controller and destroy or return existing copies. To the extent that return or destruction/deletion is infeasible or impermissible, Data Processor will continue to meet the obligations set forth in this Addendum with respect to such Personal Data and will use it only for the purpose for which it has been kept, such as to meet legal retention requirements.

2.10 The parties agree that the certification of deletion of Personal Data shall be provided by Data Processor to Data Controller upon Data Controller’s written request.

2.11 **Cooperation with Data Subject Requests.** Data Processor shall, to the extent legally permitted, promptly notify Data Controller if Data Processor receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("Data Subject Request"). Taking into account the nature of the Processing, Data Processor shall assist Data Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Data Controller's obligation to respond to a Data Subject Request under Privacy Laws. In addition, to the extent Data Controller does not have the ability to address a Data Subject Request, Data Processor shall upon Data Controller's request provide commercially reasonable efforts to assist Data Controller in responding to such Data Subject Request, to the extent Data Processor is legally permitted to do so and the response to such Data Subject Request is required under Privacy Laws. To the extent legally permitted, Data Controller shall be responsible for reasonable costs arising from Data Processor's provision of such assistance.

2.12 **Use of third party sub-processors**. Pursuant to GDPR Article 28(2) or Clause 5(h) of the SCCs, Customer acknowledges and expressly agrees that Data Processor may engage third party subprocessors in connection with the services provided pursuant to the Agreement. The current list of third party subprocessors can be found in Appendix 3 of the SCCs. Customer expressly agrees to use of the existing third party subprocessors identified in Appendix 3 of the SCCs.

2.13 Data Processor will provide Customer with notification of any new third party subprocessors. If Customer has a reasonable basis to object to Data Processor's use of a new third party subprocessor, Customer shall notify Data Processor promptly in writing within ten (10) business days after receipt of Data Processor's notice.

2.14 Data Processor shall enter into a data processing agreement with each relevant third party subprocessor. The data processing agreement shall impose the same data protection obligations on the third party subprocessor as Data Processor is subject to under this Addendum and the Agreement. Where the third party subprocessor fails to fulfil its data protection obligations, Data Processor shall remain fully liable to the Customer for the performance of the third party subprocessor's obligations.

2.15 **Updates and amendments.** The parties agree to amend this Addendum or the SCCs attached as Schedule 1 as necessary to reflect any changes or amendments to the SCCs or in the event that such SCCs are invalidated by the Commission or any competent authority.

2.16 **Limitations of liability.** The limitation of liability set forth in the Agreement remains in full force and effect and applies to this Addendum.

2.17 **Entire agreement.** This Addendum, including and together with any related schedules, appendices, and the applicable terms of any Agreement, constitutes the sole and entire agreement of the Parties with respect to the subject matter contained herein and therein, and supersedes all prior and contemporaneous understandings, agreements, representations, and warranties, both written and oral, with respect to such subject matter.

Customer

Name (written out in full):

Position:

Address:

Signature: ……………………………………….

Date: _____________________

Deltek, Inc.

Name (written out in full):

Position:

Address: 2291 Wood Oak Drive, Herndon, VA 20171 U.S.A.

Signature: ……………………………………….

Date: ________________________________

Schedule 1
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC and/or Article 46(2) of the GDPR for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, _________________________ [Insert Name and Address of Customer] (the "**data exporter"**) and Deltek, Inc., 2291 Wood Oak Drive, Herndon, Virginia, 20171, U.S.A. and its affiliated entities who are also signatories to the following Contractual Clauses (the "**data importer"**), each a "party;" together "the parties,"

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 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[1];

(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 subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor 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.

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

Clause 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 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

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 (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

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. The data subject can enforce against the subprocessor 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 subprocessor shall be limited to its own processing operations under the Clauses.

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.

Clause 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 to this contract;

(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 subprocessor 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 subprocessing 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 subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor 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).

Clause 5

Obligations of the data importer[2]

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;

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 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 subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 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 subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

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 subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor 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 of 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 subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor 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 subprocessor agrees that the data subject may issue a claim against the data subprocessor 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 subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

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.

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.

Clause 8

Cooperation with supervisory authorities

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.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, 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.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

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

Clause 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 Clause.

Clause 11

Subprocessing

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 subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[3]. Where the subprocessor 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 subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor 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 paragraph 1 of Clause 6 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 subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing 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.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor 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.

[3] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

2. The data importer and the subprocessor 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 1.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding

Signature …………………………………….

(stamp of organisation)

On behalf of the data importer:

Deltek, Inc.

Name (written out in full):

Position:

Address: 2291 Wood Oak Drive, Herndon, VA 20171 U.S.A.

Other information necessary in order for the contract to be binding (if any):

Signature…………………………………….

(stamp of organisation)

Deltek Systems (Philippines), Ltd.

Name (written out in full):

Position:

Address: The Enterprise Center, Tower 1, 6676 Ayala Ave., 6th Floor, Makati City, Philippines

Other information necessary in order for the contract to be binding (if any):

Signature…………………………………….

(stamp of organisation)

Deltek Australia PTY LTD.

Name (written out in full):

Position:

Address: Northpoint Tower, Level 40, 100 Miller Street, North Sydney, NSW 2060, Australia

Other information necessary in order for the contract to be binding (if any):

Signature…………………………………….

(stamp of organisation)

WorkBook APAC Ltd.

Name (written out in full):

Position:

Address: 53/10 Trần Khánh Dư, Phường Tân Định, Quận 1, Thành phố Hồ Chí Minh, Vietnam

Other information necessary in order for the contract to be binding (if any):

Signature…………………………………………….

(stamp of organisation)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter is (please specify briefly your activities relevant to the transfer):

Data exporter is the entity that has executed the Standard Contractual Clauses as data exporter and its associated affiliates within the EEA and Switzerland that have entered into agreements with data importer.

Data importer
The data importer is (please specify briefly activities relevant to the transfer):

Deltek, Inc., Deltek Australia PTY LTD., WorkBook APAC Ltd., and Deltek Systems (Philippines), Ltd. that have entered into agreement with data exporter to provide on-premise and/or cloud based software applications and customer support, and may Process Personal Data upon the instruction of data exporter in accordance with the terms of the Agreement.

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

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners, and vendors of Customer;
- Employees or contact persons of Customer's prospects, customers, business partners, and vendors;
- Employees, contractors, agents, vendors and advisors of Customer; or
- Customer's users authorized by Customer to use the Services.

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

- First and last name
- Title
- Position
- Employer
- Contact information
- ID data
- Professional life data
- Personal life data

Special categories of data (if appropriate)
The Personal Data transferred concern the following special categories of data (please specify):

Data exporter may choose to submit special categories of data, the extent of which is determined and controlled by data exporter in its sole discretion, and which is for the sake of clarity Personal Data with information revealing racial or ethnic origin, health information, insofar as it relates to absences, political opinions, religious or philosophical beliefs, trade-union membership, and the Processing of data concerning health or sex life.

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 services pursuant to the Agreement.
Data importer may engage subprocessors to provide parts of the services. Data importer will endeavour to reasonably ensure that subprocessors only access and use data exporter's Personal Data to provide the services and not for any other purpose.

Deltek will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality, and integrity of Personal Data transferred to Deltek, Inc., its affiliates, and/or its entities as provided in the Agreement. Additional documentation may be made reasonably available by data importer.

The following security measures relate to data importer's SaaS Infrastructure:

Audits & Certifications

Data importer's SaaS control environment for security and availability undergoes an independent evaluation in the form of SOC 1 (SSAE 18) and SOC 2 reports for Ajera, Ajera CRM, Conceptshare, Costpoint, Costpoint Enterprise, DPS / Vantagepoint, GovWin, Deltek Collaboration (f/k/a Kona), Maconomy, Maconomy Enterprise, Project Information Management, Talent Management, TrafficLIVE, Vision, Vision Enterprise and Workbook. Data importer's most recent SOC 1 and SOC 2 reports are available upon request from your organization's Deltek account executive.

Additionally, data importer's SaaS environments undergo security assessments by data importer's internal security personnel and third parties and include infrastructure vulnerability assessments and application security assessments on at least an annual basis.

Security Procedures and Policies

All data importer employees are required to abide with Deltek's Corporate Security Policies. Data importer operates in accordance with the following procedures to enhance security:

- Data importer employees must adhere to Deltek's Corporate Password Policy that requires unique passwords that must be updated regularly and are restricted from sharing
- Data importer has documented policies and procedures in place that address authorization, access control, privileges, monitoring, and revoking access to data importer's SaaS applications and associated infrastructure
- Data importer follows strict Change Management Processes that addresses risk, justification, testing, contingencies, communication, and authorization in a standardized Process to ensure minimal impact to our customers
- Data importer holds quarterly internal access audits to ensure proper access rights are observed
- Upon retirement or termination of employee, access is immediately terminated

Incident Management

Data importer maintains security incident management policies and procedures that detail how data importer identifies, reports, and responds to an incident. Data importer promptly notifies impacted customers of any actual or reasonably suspected unauthorized disclosure of their respective Customer Data by data importer or its agents of which data importer becomes aware and in compliance with applicable laws.

User Authentication

Access to data importer’s application and network platforms is restricted and secured through the use of unique username and passwords as well as multi-factor authentication (MFA), thereby ensuring access to only properly authorized personnel.

Physical Security

Data importer’s work facilities are secured and access is restricted for high-security areas. Employees wear badges and must either scan the badge or enter access codes for entry. Visitors must register prior to entry.

Visitors are not permitted at production data centers. These data centers are housed in non-descript facilities with access strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Access to data center floors are further restricted by requiring two-factor authentication for authorized staff. All physical access is logged and audited routinely.

The data centers employ automatic fire detection and suppression equipment that utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems.

The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide back-up power for the entire facility.

Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data centers are conditioned to maintain atmospheric conditions at optimal levels. Personnel and systems monitor and control temperature and humidity at appropriate levels.

Customer Data

Data importer Processes Customer Data to fulfil the products and services purchased by the Customer and as requested or instructed by the Customer. Some of the Processing activities are hosting and storing the data, providing access to the data, and providing relevant services including requests for maintenance and troubleshooting.

Data importer uses industry-accepted encryption products to protect Customer Data and communications during transmissions between a customer's network and data importer, including 128-bit TLS Certificates and 2048-bit RSA public keys at a minimum. Additionally, during replication, Customer Data is encrypted during transmission between data centers.

Each of data importer k’s various SaaS applications take daily, weekly, and monthly backups and are retained for at least 180 days and up to 12 months, depending on the applicable record retention time periods.

Upon termination of the contract, Customer Data submitted to data importer during utilization of data importer’s products and services is retained in an inactive status under applicable record retention practices. In accordance with Data importer’s backup practices, Customer Data, including inactive data, will be stored on backup. This process is subject to applicable legal requirements.

Disaster Recovery

Data importer has disaster recovery plans in place for each product offering and tests them at least once per year. Data importer's SaaS products utilize secondary facilities that are geographically remote from their primary data centers, along with required hardware, software, and Internet connectivity, in the event production facilities at the primary data centers were to be rendered unavailable.

Cybersecurity

Data importer utilizes access controls and endpoint security software that scans application files and file systems for malware including customer-supplied attachments. However, customer attachments are not scanned during the upload process.

Disclosure Control

All access to data importer's production networks is over encrypted protocols. All access to data exporter provided information is limited to employees who require that specific access.

Input Control

End users have the ability to view and report on entered data.

Segregation Control

Except for GovWin IQ, Deltek Collaboration (f/k/a Kona), and TrafficLIVE customers, each data importer client has its own separate database. A superior access is not possible.

The following security measures relate to data importer's corporate infrastructure:

Network Security

Data importer employs multiple layers of network devices and intrusion detection to protect its external attack surface. The data importer considers potential attack vectors and incorporates appropriate purpose built technologies into external facing systems.

Data importer employs multiple layers of network protection devices, including firewalls and intrusion detection. Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents.

Data importer monitors a variety of communication channels for security incidents and the data importer's security personnel will react promptly to known incidents.

Data importer utilizes access controls and endpoint security software that scans application files and file systems for malware including customer-supplied attachments.

Data importer uses industry-accepted encryption products to protect Personal Data and communications during transmissions between a customer's network and data importer, including 128-bit TLS Certificates and 2048-bit RSA public keys at a minimum.

Personnel Security

The data importer personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. The data importer conducts reasonably appropriate backgrounds checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.

Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, the data importer's confidentiality and privacy policies. Personnel are provided with security training. Personnel handling customer data are required to complete additional requirements appropriate to their role (e.g., certifications). The data importer's personnel will not Process customer data without authorization.

Subprocessor Security

Prior to onboarding subprocessors, the data importer conducts an audit of the security and privacy practices of subprocessors to ensure subprocessors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once the data importer has assessed the risks presented by the sub-processor, the subprocessor is required to abide by appropriate security, confidentiality, and privacy contract terms.

Under select circumstances, typically at the behest of data exporter, Personal Data may become accessible to data importer customer support personnel in their administration of customer support operations.

Data Privacy Office

The Data Privacy Office of data importer can be contacted by data exporter's administrators at privacy@deltek.com.

Appendix 3 to the Standard Contractual Clauses

Identification of Third Party Subprocessors

Data importer controls access to the infrastructure that stores and Processes customer data used by data importer's SaaS products. Each of data importer's SaaS products contain multiple servers and services to deliver applications efficiently and effectively. Most data importer SaaS products are hosted in a primary Amazon Web Service (AWS) region while backups are replicated to a secondary geographic region within the AWS Cloud (see asterisk(*) below the table for more information).

Additional Processing may be conducted by the following third party subprocessors: AWS, IBM, Dropbox, Hetzner Online GmbH, Microsoft, Citrix, Google, Salesforce, Oracle, Curo, Gainsight, Aria, Docusign, ZenDesk, Pendo, New Relic, Cybersource, First Capital, Stripe, Jira, LogMeIn, DUO, Sophos, Proofpoint, Progress, Optiv, Lithium, SendGrid, Pusher, Smart Software, and/or Cornerstone.

PRODUCT	PRIMARY	SECONDARY
Ajera	United States	United States
Avitru / MasterSpec	United States	United States
ConceptShare*	United States	United States
Costpoint Essentials	United States	United States
Costpoint Foundations	United States	United States
Deltek Talent Management – US	United States	United States
Deltek Talent Management – CA	Canada	Canada
Deltek Talent Management – EU	Germany	Ireland
GovWin*	United States	United States
Kona / Deltek Collaboration	United States	United States
Maconomy Enterprise – EU	Ireland	Germany
Maconomy Enterprise – NA	United States	United States
Maconomy Enterprise – APAC	Singapore	Australia
Maconomy Essentials/Flex – EU (Versions 2.4.X, 2.2.4, 2.2.1, X1)	Ireland	Germany
Maconomy Essentials/Flex – NA	United States	Ireland
Project Information Management – NA	United States	United States
Project Information Management – EU	Ireland	Germany
TrafficLIVE	Ireland	Germany
Vision / DPS / Vantagepoint – NA	United States	Ireland and United States
Vision / DPS / Vantagepoint – ANZ	Australia	Singapore
Vision / DPS / Vantagepoint – EU	Ireland	Germany
Vision Enterprise – NA	United States	United States
Vision Enterprise – EU	Ireland	Germany
WorkBook – EU*	France	Denmark and Germany
WorkBook – APAC*	Hong Kong	Hong Kong

*ConceptShare uses data centers provided by Microsoft Azure.

*GovWin uses data centers provided by Equinix.

*WorkBook uses data centers provided by IBM Softlayer and Microsoft Azure.

All customers are subject to subprocessing by Oracle for customer support and maintenance purposes. All customers are subject to subprocessing by Salesforce and Docusign for customer relationship management purposes. Additional third party subprocessing is completed as required to deliver the Services.