HOW TO EXECUTE THIS DPA:

1. This Data Processing Addendum ("DPA") consists of the following:
   a. Main body of the DPA including Annex A detailing the Technical and Organizational Security Measures implemented by Deltek;
   b. Annex B containing Model Clauses for compliance with the General Data Protection Regulations ("GDPR");
   c. Annex C containing the UK Addendum to the EU Standard Contractual Clauses;
   d. Annex D containing the Switzerland Addendum to the EU Standard Contractual Clauses.

2. This DPA has been pre-signed on behalf of Deltek.

3. Customer must complete the information in the signature box and sign on page 8.

4. Section A "Data Exporter" information on page 24 and Section B "Categories of Personal Data transferred" on page 25 of Appendix 1 to Annex B should be completed by the customer in addition to signature on page 8.

5. Customer shall send the filed up and signed DPA to Deltek by email to legal@replicon.com.

6. Except as otherwise expressly provided in the Agreement, this DPA will become legally binding upon receipt by Deltek of the validly completed DPA at the email address specified above. For the avoidance of doubt, signature of the DPA on page 8 shall be deemed to constitute signature and acceptance of the Annexes A through C as applicable.

Deltek

Data Processing Addendum for Customers

This Data Processing Addendum ("**DPA**") is effective as of the last date of signature and forms an integral part of the Master Services Agreement or the Terms and Conditions available at https://www.replicon.com/terms-and-conditions/, as may be applicable, governing the use of Deltek's proprietary cloud based Software and Service as more specifically identified on the applicable Order Forms (hereinafter jointly referred to as "**Agreement**") signed between Customer and Deltek ("**Deltek**"). All capitalized terms not defined in this DPA shall have the meaning as set forth in the Agreement.

1. DEFINITIONS

1.1 "**Affiliate**" means an entity that directly or indirectly Controls, is Controlled by or is under common Control with either party.

1.2 "**Control**" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The term "**Controlled**" will be construed accordingly.

1.3 **"Data Protection Laws"** means all data protection and privacy laws applicable to the processing of Personal Data under the Agreement, including, where applicable, EU Data Protection Lawand the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq., including any amendments and any implementing regulations including the California Privacy Rights Act of 2020 and any Data Protection Laws modelled on either of the foregoing (the "CCPA").

1.4 "**Data Controller**" means an entity that determines the purposes and means of the processing of Personal Data.

1.5 "**Data Processor**" means an entity that processes Personal Data on behalf of a Data Controller.

1.6 **"EU Data Protection Law"** means all laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the European Union, European Economic Area and the UK, including: (i) the Data Protection Act 2018; (ii) The United Kingdom 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, as modified by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 ("UK GDPR"); (iii) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ("GDPR") and (iv) the Swiss Federal Act on Data Protection as may be amended from time to time ("FADP"); and any Data Protection Laws modelled on any of the foregoing.

1.7 "**Group**" means any and all Affiliates that are part of an entity's corporate group.

1.8 "**Model Clauses**" means the Standard Contractual Clauses for Data Processors as approved by the European Commission in the form in the C(2021) 3972 final Annex to the Commission Implementing Decision 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 and in the form set out in Annex B.

1.9 "**Personal Data**" means any information which (i) identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household; or (ii) is relating to an identified or identifiable natural person.

1.10 "**Processing**" has the meaning given to it in the GDPR and "**process**", "**processes**" and "**processed**"

will be interpreted accordingly.

1.11 "**Security Incident**" means any breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data.

1.12 "**Special Categories of Personal Data**" means the processing of biometric data in the form of photographs by Deltek or its Affiliates for the purpose of fulfilling its obligations with respect to providing the Service pursuant to the Agreement or this DPA.

1.13 "**Sub-processor**" means any Data Processor engaged by Deltek or its Affiliates, subject always to Deltek observing Section 4 (Sub-processing) of this DPA, to assist in fulfilling its obligations with respect to providing the Service pursuant to the Agreement or this DPA.

2. SCOPE OF THIS DPA

2.1 **Scope of DPA:** This DPA applies where and only to the extent that Deltek processes Customer Data or Personal Data on behalf of Customer in the course of providing the Service to the Customer pursuant to the Agreement. References to Customer Data in this DPA shall include all Personal Data that Deltek processes on behalf of the Customer pursuant to the Agreement.

2.2 The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects whose Personal Data will be Processed under this DPA are further specified in Section 3 below.

3. ROLES AND SCOPE OF PROCESSING

3.1 **Role of the Parties:** As between Deltek and Customer, Customer or any of its Affiliates is the Data Controller of Customer Data and Deltek shall process Customer Data only as a Data Processor acting on behalf of Customer.

3.2 **Customer Processing of Customer Data:** Customer agrees and undertakes that it will comply with its obligations as a Data Controller under applicable Data Protection Laws in respect of its processing of Customer Data and any processing instructions it issues to Deltek.

3.3 **Deltek Processing of Customer Data:** As a Data Processor, Deltek shall treat Customer Data as confidential information and will process Customer Data only for the purpose of providing the Service and in accordance with Customer's documented lawful instructions, as set forth in the Agreement and this DPA. The parties agree that the Customer's complete and final instructions with regard to the nature and purposes of the processing are set out in this DPA and the Agreement. Processing outside the scope of these instructions will require prior written agreement between Customer and Deltek with additional instructions for processing.

3.4 Deltek shall treat the Personal Data as confidential information under the Agreement (except that any exclusion from the definition of Confidential Information in the Agreement will not apply to Personal Data). Other than as expressly permitted by this DPA or by Data Protection Laws, Deltek shall not disclose, transfer or otherwise make available Personal Data in exchange for monetary or other valuable consideration to any third parties and shall not combine the Personal Data it Processes on behalf of Customer with any other information it collects from any other customers of Deltek.

3.5 **Details of Data Processing:**

Subject matter: The subject matter of the data processing under this DPA is the Customer Data.

Duration: As between Deltek and Customer, the duration of the data processing under this DPA is the term of the Agreement and the subsequent data retention period as enumerated in Section 8

of this Agreement.

Purpose: The purpose of the data processing under this DPA is the provision of the Service by Deltek to the Customer.

Nature of the processing: Deltek provides a cloud-based time intelligence platform ("**Platform**") which enables its customers to collect and harness time data, and other such professional services as described in the Agreement. Deltek processes Customer Data upon the instruction of Customer in accordance with the terms of the Agreement.

Categories of Data Subjects: The categories of Data Subjects are specified in the Description of Transfer section in Part B of Appendix 1 to Annex B hereunder.

Types of Customer Data: The types of Customer Data are specified in the Description of Transfer section in Part B of Appendix 1 to Annex B hereunder.

Special Categories of Personal Data: The types of Special Categories of Personal Data are specified in the Description of Transfer section in Part B of Appendix 1 to Annex B hereunder.

3.6 **Prohibited Data**: Except as expressly disclosed in Section 3.5 (Details of Processing) above and in the Description of Transfer section in Part B of Appendix 1 to Annex B hereunder, Customer and its Affiliates shall not disclose (and shall not permit any data subject to disclose) any Sensitive Personal Data to Deltek by any means, including but not limited to information submitted through custom field extensions within the Service, for processing by Deltek. Where Sensitive Personal Data except as expressly disclosed in Section 3.5 (Details of Processing) above and in the Description of Transfer section in Part B of Appendix 1 to Annex B hereunder, is nevertheless submitted within Customer Data, Customer and its Affiliates acknowledge that the processing of such Sensitive Personal Data shall be considered beyond the scope of this DPA and Customer and its Affiliates accept full responsibility for any subsequent liability arising from the processing of such unauthorized Sensitive Personal Data.

4. SUBPROCESSING

4.1 **Authorized Sub-processors**: Subject to the provisions of this section, Customer acknowledges and agrees that, Deltek may engage Sub-processors to process Customer Data. Deltek maintains an up-to-date list of its authorized Sub-processors, available on the following link: www.replicon.com/resource/subprocessors.

4.2 **Sub-processor Obligations**: Where Deltek authorizes any Sub-processor as described in Section 4.1:

(a) Deltek shall carry out adequate due diligence on the Sub-processor to ensure it is capable of providing the level of protection of Personal Data required by this DPA;

(b) Deltek will restrict the Sub-processors access to only the requisite Customer Data necessary to assist Deltek in providing or maintaining the Service, and prohibit the Sub-processor from accessing Customer Data for any other purpose;

(c) Deltek will enter into a written agreement with the Sub-processor imposing data protection terms that require the Sub-processor to protect the Customer Data to the standard required by Data Protection Laws and this DPA; and

(d) Deltek will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause Deltek to breach any of its obligations under this DPA.

4.3 Deltek will provide Customer with at least 45 days' prior written notice on its website www.replicon.com/resource/subprocessors as well as on email to an email address specified by the Customer of any proposed changes to its Sub-processors. Customer may object in writing to Deltek's appointment of a new, or replacement of an old, Sub-processor within fifteen (15) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties will discuss such concerns in good faith with a view to achieving resolution. If this is not possible, Customer may terminate the Agreement (without prejudice to any fees incurred by Customer prior to the effective date of such termination and Deltek shall provide Customer a pro-rata refund, within thirty (30) days from the effective date of termination, of any prepaid fees for the unused portion of the Service calculated from the effective date of termination).

5. SECURITY MEASURES AND SECURITY INCIDENT RESPONSE

5.1 **Security Measures**: Deltek has implemented and will maintain appropriate technical and organizational security measures to protect Customer Data from Security Incidents and to preserve the security and confidentiality of the Customer Data ("**Security Measures**"). The Security Measures applicable to the Service are set forth in Annex A, as updated or replaced from time to time in accordance with Section 5.2.

5.2 **Updates to Security Measures**: Customer acknowledges that the Security Measures are subject to technical progress and development and Deltek may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Service purchased by the Customer.

5.3 **Personnel:** Deltek restricts its personnel from processing Customer Data without prior authorization as set forth in the Security Measures and shall ensure that any person who is authorized by Deltek to process Customer Data is under an appropriate statutory or contractual obligation of confidentiality.

5.4 **Customer Responsibilities**: Notwithstanding the above, Customer agrees that the Customer is responsible for securing its account authentication credentials and taking appropriate steps to securely encrypt or backup Customer Data prior to it being uploaded to the Service and for Customer Data that has been downloaded or transferred from the Service.

5.5 **Security Incident Response:** Upon becoming aware of a Security Incident, Deltek will notify Customer without undue delay (in any case no later than 72 hrs. from the time Deltek becomes aware) and will provide information relating to the Security Incident as it becomes known or as is reasonably requested by Customer. Deltek will also take reasonable steps to mitigate and, where possible, to remedy the effects of, any Security Incident.

6. AUDIT REPORTS

6.1 **Audit Reports:** Deltek audits its compliance against data protection and information security standards on a regular basis through independent, experienced personnel, which may include Deltek's internal audit team and/or third party auditors engaged by Deltek. Upon Customer's prior written request, Deltek will provide the details of the audits relevant to the Service being provided to the Customer and, if required, supply Customer with the most recent SSAE 18 SOC Type II audit report (or comparable industry standard third party report or certification (**"Report"**).

6.2 **Confidentiality of Audit Reports**: The Customer acknowledges that each Report is Deltek's Confidential Information and Customer shall protect the Report in accordance with the confidentiality provisions of the Agreement.

6.3 **Audit and Inspection Right.** To the extent required by Data Protection Laws, the Model Clauses, in the event of a Security Incident or if required to respond to a regulator, Deltek shall promptly and adequately make available to Customer and any regulator, on request, all information

necessary to demonstrate its compliance with this DPA. Deltek shall allow for audits and inspections by any regulator in order to assess its compliance with this DPA. A prior written notice of at least fifteen (15) days has to be provided if an audit or inspection is to conducted by Customer or an auditor mandated by Customer or any of its Affiliates with the scope, timing, cost and duration to be mutually agreed between Deltek and Customer prior to commencement of the audit. Customer shall promptly share the final report detailing the findings of such audit for Deltek records. Deltek shall immediately inform Customer if, in its opinion, an instruction pursuant to this Section infringes any Data Protection Laws.

7. TRANSFERS OF PERSONAL DATA

7.1 **Data center locations:** For the sole purpose of rendering the Service, Deltek offers multiple data hosting locations to Customer for hosting Customer Data as per the choice of Customer or its Affiliate. If the Customer does not nominate a specific data hosting location from the list of Deltek data hosting locations, Deltek will select one of its available data hosting locations that in its sole discretion and judgement finds most conducive in adhering to Data Protection Laws.

7.2 **Application of Model Clauses**: The Model Clauses will apply, by incorporation into this DPA, to Customer Data that originates inside the European Economic Area (including United Kingdom subject to Annex C – UK Addendum to the EU Standard Contractual Clauses) ("**EEA**"), and/or Switzerland and that is transferred outside the EEA and/or Switzerland (subject to Annex D – Switzerland Addendum to the EU Standard Contractual Clauses), either directly or via onward transfer, to any country not recognized by the UK or European Commission or Swiss Federal Data Protection Authority (as applicable) as providing an adequate level of protection for Personal Data (as described in the GDPR).

7.3 Deltek shall support Customer to ensure compliance with Data Protection Laws and other applicable law for the transfer of Personal Data of Data Subjects located in the UK, Switzerland or the EEA to third countries including by undertaking and documenting a transfer risk assessment in accordance with Data Protection Laws and the Model Clauses before first transferring Personal Data and then no less than annually and Deltek shall deliver such completed transfer risk assessment promptly to Customer upon prior written request.

7.4 Deltek shall ensure that the appropriate technical and organizational measures it implements and maintains as required by the Standard Contractual Clauses, address the risks associated with the transfer of Personal Data to a third country and Deltek shall implement any further additional safeguards required by its transfer risk assessment and/or as agreed with Customer.

7.5 Deltek warrants on an ongoing basis that it is able, through the implementation of appropriate technical and organizational measures, to satisfy its obligations under the Model Clauses and this DPA.

7.6 Deltek certifies that: (i) it has not and will not create back doors (non-transparent access capabilities) or similar programming that could be used to access its systems and/or the Personal Data; (ii) it has not and will not change its business processes in a way which facilitates unauthorized access to its systems and/or the Personal Data; and (iii) applicable law does not require Deltek to create or maintain back doors or to facilitate unauthorized access to its systems and/or the Personal Data or for Deltek to be in possession of or to hand over to any third party keys to decrypt the Personal Data.

8. RETURN OR DELETION OF DATA

8.1 Following expiration of the Agreement, Deltek shall retain Customer Data for a period of up to thirty (30) days and thereafter permanently delete all Customer Data including Personal Data in its possession in accordance with the terms of the Agreement save to the extent Deltek may be

required by applicable Data Protection Laws to retain some or all of the Customer Data and Personal Data (in which case, Deltek shall isolate the Customer Data from any further processing), continue to protect it in accordance with this DPA and delete it as soon as permitted by applicable Data Protection Laws). Deltek shall provide a written letter or certificate of destruction upon prior written request of Customer.

9. COOPERATION

9.1 The Service provides Customer with necessary controls to retrieve, correct, delete or restrict Customer Data, which Customer may use in connection with its obligations under the Data Protection Laws, including its obligations relating to responding to requests from Data Subjects or applicable data protection authorities. If Customer does not use the controls provided within the Service to retrieve, correct, delete or restrict Customer Data and makes manifestly unfounded or excessive requests to Deltek to retrieve, correct, delete or restrict Customer Data, in particular because of the repetitive character of the Customer requests, as more specifically detailed in Article 12 (5) of the GDPR, Deltek reserves the right to either a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested by the Customer or b) refuse to act on the request. If the Customer is unable to access the relevant Customer Data within the Service due to technical errors or due to limitations in the Service, Deltek shall provide reasonable assistance to Customer to respond to any requests or complaints from individuals or applicable data protection authorities relating to the processing of Personal Data under the Agreement. If any such request is made directly to Deltek, without Customer's prior authorization, Deltek shall not respond to such communication directly, unless legally compelled to do so. If Deltek is legally compelled to respond to such a request, Deltek will promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

9.2 If a law enforcement agency sends Deltek a demand for Customer Data (for example, through a subpoena or court order), Deltek will redirect the law enforcement agency to request that data directly from Customer. As part of this effort, Deltek may provide Customer's basic contact information to the law enforcement agency. If compelled to disclose Customer Data to a law enforcement agency, Deltek will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Deltek is legally prohibited from doing so.

9.3 To the extent Deltek is required under Data Protection Laws, Deltek will provide reasonably requested information regarding the Service and assistance to enable the Customer to carry out data protection impact assessments and prior consultations with data protection authorities as required by law.

10. GENERAL

10.1 The parties agree that this DPA shall replace and supersede any existing DPA (including the Model Clauses (as applicable)) the parties may have previously entered into in connection with the Service.

10.2 Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect, including, but not limited to, the mutual indemnities provided by the parties. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict.

10.3 For the avoidance of doubt, any claim or remedies the Customer may have against Deltek, any of its Affiliates and their respective employees, agents and sub-processors arising under or in connection with this DPA, including: (i) for breach of this DPA; (ii) as a result of fines (administrative, regulatory or otherwise) imposed upon Customer; and (iii) breach of its obligations under the Model Clauses, except for damages due to a data subject which cannot be

so limited by applicable Data Protection Laws, will be subject to any limitation of liability provisions (including any agreed aggregate financial cap) that apply under the Agreement. Customer further agrees that any regulatory penalties incurred by Deltek in relation to the Customer Data, that arise as a result of, or in connection with, Customer's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce Deltek's liability under the Agreement as if it were liability of the Customer under the Agreement.

10.4 No one other than a party to this DPA, their successors and permitted assignees shall have any right to enforce any of its terms**.**

10.5 This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

10.6 The provisions of this DPA are severable. If any phrase, clause or provision is invalid or unenforceable in whole or in part, such invalidity or unenforceability shall affect only such phrase, clause or provision, and the rest of this DPA shall remain in full force and effect.

10.7 This DPA and the Model Clauses will terminate simultaneously and automatically with the termination or expiry of the Agreement or the deletion of Customer Data by Deltek whichever is later.

IN WITNESS WHEREOF, the parties have caused this DPA to be executed by their authorized representative effective as at the date of the last signature.

DELTEK	Customer
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____

ANNEX A

TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES IMPLEMENTED BY DELTEK

Deltek has implemented and maintains the controls listed here in accordance with industry standards generally accepted by information security professionals, e.g. SSAE 18 SOC 1, SSAE SOC 2, FedRAMP (NIST SP800-53r4) and ISO/IEC 27001:2013, Microsoft Security Hardening Guides, OWASP Guide to Building Secure Web Applications, and the various Center for Internet Security Standards etc., as necessary to reasonably protect Personal Data during storage, processing and transmission.

Capitalized terms used and not defined in this attachment have the meanings given in the DPA or elsewhere in the relevant Agreement.

Security Control Category	Description
Information Security Program	• Assign to an individual or a group of individuals the responsibility for developing, implementing, and managing a comprehensive written information security program for the organization; • The relevant personnel must be sufficiently trained, qualified and experienced to be able to fulfill these functions and any other functions that might reasonably be expected to be carried out by the personnel responsible for safeguarding Personal Data; • Develop, maintain and document reasonable technological, physical, administrative and procedural safeguards, including without limitation, policies, procedures, guidelines, practices, standards, and controls that: – Ensure the privacy, confidentiality, security, integrity and availability of Personal Data; – Protect against any anticipated threats or hazards to the security and integrity of Personal Data; – Protect against any Security Incident. • Regularly test, and monitor and evaluate the sufficiency and effectiveness of the information security program, including Security Incident response procedures.
Risk Assessment	• Conduct information security risk assessments at least annually and whenever there is a material change in the organization's business or technology practices that may impact the privacy, confidentiality, security, integrity or availability of Personal Data; • The risk assessment should include: – Identifying and assessing reasonably foreseeable internal and external threats and risks to the privacy, confidentiality, security, integrity and availability of Personal Data; – Assessing the likelihood of, and potential damage that can be caused by, identified threats and risks; – Assessing the adequacy of personnel training concerning, and compliance with, the organization's information security program; – Assessing the adequacy of service provider arrangements; – Adjusting and updating the organization's information systems and information security program to limit and mitigate identified threats and risks, and to address material changes in relevant technology, business practices, Personal Data practices and sensitivity of Personal Data the organization processes; – Assessing whether the organization's information security program is operating in a manner reasonably calculated to prevent and mitigate Security Incidents;

	• Documenting the risk assessment; • Risk assessments should be conducted by independent third parties or internal personnel independent of those who develop or maintain the organization's information systems or information security program.
Data Collection, Retention and Disposal	• Collect only as much Personal Data as needed to accomplish the purpose for which the information is collected; • Refrain from storing Personal Data on media connected to external networks unless necessary for business purposes; • Prohibit download and use of file sharing and other software that can open security vulnerabilities to areas or systems that hold Personal Data; • Securely dispose of records containing Personal Data so that the information cannot be read or reconstructed after it is no longer needed to comply with business purposes or legal obligations; • Securely erase media containing Personal Data before reuse.
Data Inventory	• Track and periodically inventory Personal Data the organization collects, uses, maintains, discloses, disposes of or otherwise processes, along with the purposes for Processing such Personal Data; • Periodically inventory the organization's information systems and assets that contain Personal Data.
Personnel Background Checks	• Conduct reasonable background checks (including criminal background checks) of any personnel or third parties who will have access to Personal Data or relevant information systems, and repeat the checks at appropriate and adequate intervals; • Maintain policy prohibiting individuals convicted of a crime of dishonesty, breach of trust or money laundering from having access to Personal Data.
Personnel Training and Education	Regularly and periodically train personnel, subcontractors and any third parties who have access to Personal Data or relevant information systems concerning: • The organization's information security program; • The importance of the security, confidentiality and privacy of Personal Data; • The risks to the organization and its customers associated with Security Incidents.
Processor Management and Oversight	• Take reasonable steps and conduct due diligence to select and retain subcontractors that are capable of maintaining the privacy, confidentiality, security, integrity or availability of Personal Data consistent with the organization's contractual and other legal obligations; • Contractually require subcontractors to maintain adequate safeguards for Personal Data that are at least equivalent to the safeguards that the organization must implement pursuant to contractual or legal requirements; • Regularly assess and monitor subcontractors to confirm their compliance with the applicable privacy and information security requirements.
Segregation of Duties	• Duties and areas of responsibility of the organization's personnel should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of Personal Data or the organization's information systems.
Access Controls	• Identify personnel, classes of personnel and third parties whose documented business functions and responsibilities require access to Personal Data, relevant information systems and the organization's premises; • Permit access to Personal Data, relevant information systems and the organization's premises only to such authorized personnel and third parties; • Maintain a current record of personnel and third parties who are authorized to access Personal Data, relevant information systems and the organization's premises, and the purposes of such access;

	• Maintain logical and physical access controls, secure user authentication protocols, secure access control methods, and firewall protection; • Prevent terminated personnel, subcontractors or other third parties from accessing Personal Data and information systems by immediately terminating their physical and electronic access to Personal Data and relevant information systems.
Secure User Authentication	To manage access to Personal Data and relevant information systems: • Maintain secure control over user IDs, passwords and other authentication Identifiers; • Require passwords controlling access to Personal Data to have minimum complexity requirements and be at least 8 characters in length; • Maintain a secure method for selecting and assigning passwords and use multifactor authentication and other reasonable authentication technologies; • Assign unique user identifications and passwords that are not Processor supplied default passwords; • Require personnel, subcontractors and other third parties to change passwords at regular intervals or based on the number of access attempts, and whenever there is any indication of possible system or password compromise; • Frequently (and at least every 90 days) change passwords for accounts that have access to Personal Data; • Avoid reusing or recycling old passwords; • Restrict access to Personal Data and relevant information systems to only active users and accounts; • Block user access after multiple unsuccessful attempts to login or otherwise gain access to Personal Data or relevant information systems; • Terminate user access after a predetermined period of inactivity; • Promptly revoke or change access in response to personnel termination or changes in job functions.
Incident Detection and Response	Maintain policies and procedures to detect, monitor, document and respond to actual or reasonably suspected Security Incidents, and encourage the reporting of such incidents, including through: • Training personnel with access to Personal Data to recognize actual or potential Security Incidents and to escalate and notify senior management of such incidents; • Mandatory post-Security Incident review of events and actions taken concerning the security of Personal Data; • Policies governing the reporting of Security Incidents to regulators and law enforcement agencies.
Encryption	Apply encryption with industry-standard algorithms and key lengths to Personal Data: • Stored on laptops, mobile devices, portable storage devices or removable archival media; • Stored on file servers or in application databases; • Stored outside of the organization's physical controls; • Transmitted across any public network (such as the Internet) or wirelessly; • Transmitted in email attachments; • In transit outside of the organization's information systems. • Maintain policies prohibiting such storage or transmission unless required encryption has been applied.

Network Security	Implement network security controls such as up-to-date firewalls, layered DMZs and updated intrusion detection/prevention systems, including firewalls between the organization's information systems, the Internet (including internal networks connected to the Internet) and other public networks, and internal networks that are not necessary for processing Personal Data; the firewalls must be reasonably designed to maintain the security of Personal Data and relevant information systems.
Data Segregation	Physical or logical segregation of Personal Data to ensure it is not comingled with another party's information except as approved by Controller.
Malicious Code Detection	• Implement and maintain software that detects, prevents, removes and remedies malicious code designed to perform an unauthorized function on, or permit unauthorized access to, any information system, including without limitation, computer viruses, Trojan horses, worms, and time or logic bombs; • Run malicious code detection software at least daily; • Update malicious code detection software at least daily, including by obtaining and implementing the most current available virus signatures.
Vulnerability and Patch Management	Maintain vulnerability management and regular application, operating system and other infrastructure patching procedures and technologies to identify, assess, mitigate and protect against new and existing security vulnerabilities and threats, including viruses, bots, and other malicious code.
Application Security	Maintain application security and software development controls designed to prevent the introduction of security vulnerabilities in software developed by Processor that Processes Personal Data.
Change Controls	• Prior to implementing changes to the organization's information systems, follow a documented change management process to assess the potential impact of such changes on privacy, confidentiality, security, integrity and availability of Personal Data, and determine whether such changes are consistent with the organization's information security program; • No changes should be made to the organization's information systems or information security program that increase the risk of a Security Incident or fail to comply with the organization's contractual or other legal obligations.
Off-Premise Information Security	• Maintain policies governing the security of the storage, access, transportation and destruction of records or media containing Personal Data outside of the organization's business premises; • Monitor and document movement of records or media containing Personal Data • Create copies of Personal Data before movement of records or media containing the information.
Physical Security	• Maintain reasonable restrictions on physical access to Personal Data and relevant information systems (e.g., clean desk policy); • Maintain physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster; • Lock workstations with access to Personal Data when unattended; • Document repairs and modifications to information security-related physical components of the organization's information systems.
Secure Destruction	Use secure destruction procedures to sanitize any unencrypted hard disk, portable storage device or backup media containing Personal Data prior to sending it offsite for maintenance or disposal purposes.

Contingency Planning	Maintain policies and procedures for responding to an emergency or other occurrence that can compromise the privacy, confidentiality, integrity or availability of Personal Data or damage the organization's information systems; such policies and procedures should provide for: • Creating and maintaining retrievable copies of Personal Data; • Restoring any loss of Personal Data; • Enabling continuation of critical business processes involving Personal Data in emergency mode; • Assessing relative criticality of specific applications and Personal Data in support of other contingency plan components; • Periodic testing and updates of contingency plans.

ANNEX B

MODEL CLAUSES

Standard Contractual Clauses (Controller- Processor)

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in An I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Appendix I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Appendix I.B.

(d) The Appendices to these Clauses form an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b);

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Appendix I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Appendix I.A.

(b) Once it has completed the Appendix and signed Appendix I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Appendix I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Appendix I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Appendix II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Appendix I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the

exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Appendix II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Appendix I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9
Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days' in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

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

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

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Appendix II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

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

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the

data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

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

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Appendix I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers;

the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation(EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

APPENDIX I

A. LIST OF PARTIES

1. **Data exporter(s):** The data exporter is the legal entity that is identified as "Customer" in the Agreement, including all Affiliates of the Customer operating in the countries which comprise the European Economic Area, Switzerland, the United Kingdom and/or in any other country which accepts the EU Standard Contractual Clauses, which are controllers and which transfer personal data to the data importer.

   Name: Click or tap here to enter text.

   Address: Click or tap here to enter text.

   Contact person's name, position and contact details: Click or tap here to enter text.

Activities relevant to the data transferred under these Clauses: As set out in the Agreement.

Signature and date: The parties agree that execution of the Agreement shall constitute execution of these Clauses by both parties.

Role (controller/processor): controller

2. **Data importer(s):**

1. Name: Deltek, Inc. and its affiliated entities: Deltek Australia PTY Ltd., Deltek GB Limited, Deltek (Systems) Canada, Inc., Deltek Systems (Philippines), Ltd. And Replicon Software (India) Private Limited.

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

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

The Aircraft Factory Cambridge House, 100 Cambridge Grove, London W6 0LE, United Kingdom;

5300 Commerce Court West, 199 Bay Street, Toronto, ON Canada M5L 1B9;

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

Mantri Commercio - Tower B, 5th Floor, Marathahalli Outer Ring Road, Devarabisanahalli, Bellandur Post, Bangalore-560103

Contact person's name, position and contact details: Jon Knight – Senior Counsel for Privacy and Security, privacy@deltek.com.

Activities relevant to the data transferred under these Clauses: The data importer provides the Services to the data exporter in accordance with the Agreement

Signature and date: The parties agree that execution of the Agreement shall constitute execution of these Clauses by both parties.

Role (controller/processor): processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

Customer may submit Personal Data to the Service, 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:

- Employees, contractors, agents, advisors, freelancers (past, potential, present and future) of Customer and its Affiliate (who are natural persons);
- Prospects, customers, business partners and vendors of Customer and its Affiliates (who are natural persons);
- Customer's Users authorized by Customer to use the Service.

Categories of personal data transferred:

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 the following categories of Personal Data:

Categories of personal data	*Strike through if not applicable*
Communication data (e.g. first name, last name, address, title, position, telephone, e-mail address, business address, contact details, etc.)	yes/no If yes, Click or tap here to enter text.
Connection data (e.g. IP address, logs, usernames, passwords, etc.)	yes/no If yes, Click or tap here to enter text.
Contractual data (e.g contractual relationship, order history, order numbers, billing and payment etc.)	yes/no If yes, Click or tap here to enter text.
Employment data (e.g. employer name, job title, geographic location, project information (including any working schedules or other similar working time related information of an employee), area of responsibility)	yes/no If yes, Click or tap here to enter text.
Official ID data (e.g. copy of passport or national ID), data related to civil status	yes/no If yes, Click or tap here to enter text.
Data pertaining to the personal life of Data Subjects (e.g. life habits, familial situation, etc.)	yes/no If yes, Click or tap here to enter text.
Data pertaining to the professional life of Data Subjects (e.g. CV, professional trainings, certifications, etc.)	yes/no If yes, Click or tap here to enter text.
Economic and Financial Data (e.g. compensation, financial status, tax situation, credit card details, account details, payment information, etc.)	yes/no If yes, Click or tap here to enter text.
Location Data (e.g. travels, GPS data, GSM data, etc.)	yes/no If yes, Click or tap here to enter text.
Any other category: Click or tap here to enter text.	yes/no If yes, Click or tap here to enter text.

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

Data Exporter may only submit special categories of Personal Data limited only to photographs for the purpose of the Service. The Service is not designed to require the submission of any other special categories of Personal Data except as defined hereinabove. To the extent any other such special categories of Personal Data is submitted to the Service, apart from those defined herein, it is determined and controlled by data exporter in its sole discretion.

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

Personal Data may be transferred on a continuous basis during the term of the Agreement as necessary to provide the Services.

Nature of the processing:

The nature of processing is set forth in Sec 3.5 of the DPA.

Purpose(s) of the data transfer and further processing

The purpose of the processing is set out in Section 3.5 of the DPA.

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

Subject to section 8 of the DPA, data importer will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

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

As per Section 4 of the DPA, the Sub-processor will Process Personal Data as necessary to perform the Services pursuant to the Agreement. The Sub-processor will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

C. COMPETENT SUPERVISORY AUTHORITY

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

- The Information Commissioner's Office (UK)
- The Data Protection Commission (Ireland)
- The Federal Data Protection and Information Commissioner (Switzerland)

APPENDIX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

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

The Technical and Organizational Security Measures are described in Annex A of the DPA.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

The Technical and Organizational Security Measures are described in Annex A of the DPA.

ANNEX C

UK Addendum to the EU Standard Contractual Clauses

This Annex forms part of and is incorporated into the Exhibit to which it is attached.

Except where otherwise defined in the Exhibit, capitalised terms used in this Annex have the meaning given to them in the Mandatory Clauses (as defined in Part 2 below in the table below).

In the event of a Restricted Transfer, the parties enter into this Addendum as issued by the ICO and as amended from time to time to the extent necessary to operate to provide Appropriate Safeguards for Restricted Transfers in accordance with Article 46 of the UK GDPR.

PART 1: TABLES	
TABLE 1	
PARTIES	The Parties are set out in Annex I A. of the Appendix to the Approved EU SCCs included under Annex B above.
TABLE 2	
SELECTED SCCS, MODULES AND SELECTED CLAUSES	The version of the Approved EU SCCs shall be the version of the EU SCCs included at Annex B above.
TABLE 3	
APPENDIX INFORMATION	Annex 1A: List of Parties: See the details for the data exporters and data importer(s) provided at Annex I A. to the Appendix of the version of the Approved EU SCCs.
	Annex 1B: Description of Transfer: See the description of transfer provided at Annex I B. of the Appendix to the Approved EU SCCs.
	Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Annex II of the Appendix to the Approved EU SCCs.
	Annex III: List of Sub processors: See the details relating to sub-processors provided at Section 4 of the DPA.
TABLE 4	
ENDING THIS ADDENDUM WHEN THE APPROVED ADDENDUM CHANGES	Neither Party shall have the right to end this Addendum pursuant to Section 19.
PART 2: MANDATORY CLAUSES	
Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses	

ANNEX D

Switzerland Addendum to the EU Standard Contractual Clauses

This Annex forms part of and is incorporated into the Exhibit to which it is attached.

Where the Standard Contractual Clauses apply to a transfer of Personal Data to which the FADP applies, the Standard Contractual Clauses shall be deemed to be amended to the extent necessary to operate to provide appropriate safeguards for such transfers in accordance with the FADP, including without limitation the following:

(i) Clause 13(a) and Part C of Annex I are not used; the "competent supervisory authority" is the Federal Data Protection and Information Commissioner;

(ii) the term "Member State" cannot be interpreted to exclude data subjects in Switzerland from exercising their rights under Data Protection Law;

(iii) the term "personal data" shall be deemed to include the data of legal entities to the extent such data is protected under the FADP; and

(iv) any amendments required from time to time by the Federal Data Protection and Information Commissioner in order to comply with the FADP.