

SUPPLIER PERSONAL DATA PROCESSING ADDENDUM

This Supplier Personal Data Processing Addendum (“**DPA**”) is between:

- The Open Text entity having entered into a written or electronic agreement, which includes any Statements of Work or similar documentation attached thereto (“**SOW**”); collectively the (“**Agreement**”) acting on its own behalf (“**OT**” or “**OpenText**”) and its Affiliates; and
- the other party to the Agreement (“**Supplier**”).

BACKGROUND

This DPA amends or supplements the Agreement provided that the Services include Processing of Personal Data, as may be described in Appendix A.

CONTENTS

1.	DEFINITIONS	2
2.	ROLES AND SCOPE OF PROCESSING	3
3.	SUPPLIER’S OBLIGATIONS	3
4.	BREACH NOTIFICATION	6
5.	SUB-PROCESSING	7
6.	AUDIT	7
7.	DELETION OF OT DATA	8
8.	INDEMNIFICATION	8
9.	LIMITATION OF LIABILITY	8
10.	GEOGRAPHICAL SPECIFIC DATA PROCESSING TERMS AND INTERNATIONAL TRANSFERS	9
11.	CONFLICT	9
12.	OTHER PROVISIONS	9

Appendices

APPENDIX A	DETAILS OF THE PROCESSING OF PERSONAL DATA
APPENDIX B	TECHNICAL AND ORGANIZATIONAL MEASURES (IT SECURITY TERMS AND CONDITIONS)
APPENDIX C	SUB-PROCESSORS AND LOCATIONS OF PROCESSING
APPENDIX D	GEOGRAPHICAL SPECIFIC TERMS
APPENDIX E	INCORPORATION OF TRANSFERS MECHANISMS
APPENDIX F	INTERNATIONAL DATA EXPORT REQUIREMENTS
APPENDIX G	TRANSFER SIGNATORY PARTIES

1. DEFINITIONS

In this DPA, the following terms shall have the meanings set out below:

- 1.1 "**Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with a party, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of management and the policies of an entity, whether through ownership of voting securities, by contract or otherwise.
- 1.2 "**Business Purpose**" means the provision of Services as set forth under the Agreement.
- 1.3 "**Data Breach**" means a breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, OpenText Data and also includes any incident classified as a "personal data breach," "data breach," or similarly defined term under Data Protection Legislation.
- 1.4 "**Data Protection Authority**" means the body officially appointed as responsible body for overseeing and/or enforcing the Data Protection Legislation, and/or promoting data privacy for individuals.
- 1.5 "**Data Protection Legislation**" means any laws, regulations, and other legal requirements, to the extent applicable to the Processing (as defined below) of Personal Data under this DPA, and the Agreement relating to (a) privacy, confidentiality and data security of Personal Data, and/or (b) the use, collection, retention, storage and security, disclosure, transfer, disposal, and/or other Processing of any Personal Data (as defined below). Notwithstanding the preceding, Data Protection Legislation does not include the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA").
- 1.6 "**New Standard Contractual Clauses**" or "**New SCCs**" means mechanisms approved or otherwise released by Data Protection Authorities or relevant governments to allow for Restricted Transfers to take place if such mechanisms are put in place between exporter and importer of the Personal Data transferred.
- 1.7 "**OpenText Data**" or "**OT Data**" means any data, whether electronic or otherwise, personal or not personal that the Supplier may process in providing the Services, including, without limitation, any data specifically pertaining to company, its affiliates, or its employees, users, partners, customers, or suppliers.
- 1.8 "**Restricted Transfer**" means an international transfer of Personal Data made in connection with the Agreement where such transfer would be prohibited by applicable Data Protection Legislation except where,
 - the jurisdiction to which the Personal Data is transferred has been approved by a competent authority as ensuring an adequate level of protection for the Processing of Personal Data under applicable Data Protection Legislation ("**Adequacy Decision**");
 - a Transfer Mechanism may be put in place in respect of the relevant Restricted Transfer.
 - the jurisdiction to which the Personal Data is transferred has been approved by the relevant authority in that jurisdiction as ensuring an adequate level of protection for the Processing of Personal Data under applicable Data Protection Legislation; or
 - a derogation that permits such transfer under applicable Data Protection Legislation applies ("**Derogation**").
- 1.9 "**Services**" means the services and other activities to be supplied or carried out by or on behalf of Supplier for OT pursuant to the Agreement.

- 1.10 “**Standard Contractual Clauses**” or “**SCCs**” means, to the extent applicable under Data Protection Legislation, model contractual clauses approved by the competent authority (as set out in the Data Protection Legislation) to ensure appropriate data protection safeguards and used as a Transfer Mechanism providing a legal ground to allow for Restricted Transfers of Personal Data.
- 1.11 “**Sub-processor**” means any third party (including, without limitation, any Supplier Affiliate) appointed by or on behalf of Supplier to Process Personal Data on behalf of OT or OT Affiliate in connection with the Agreement.
- 1.12 “**Technical and Organizational Measures**” means the technical and organizational measures for the relevant Service set out in Appendix B, as may be amended, updated, or replaced from time to time.
- 1.13 “**Third Country**” means any country, organization or territory that have not been granted with an Adequacy Decision by the relevant Data Protection Authority or an authorised government body.
- 1.14 “**Transfer Mechanism**” means the Standard Contractual Clauses and/or any other contractual mechanism, Adequacy Decision, Derogation and any other solution incorporated by Data Protection Legislation to allow Restricted Transfers to take place.
- 1.15 The terms “**Controller**”, “**Data Subject**”, “**Personal Data**”, “**Processing**”, “**Process**” and “**Processor**”; “**Sell**”, “**Sensitive Personal Data**”, “**Service Provider**”, “**Share**” have the same meaning as in the applicable Data Protection Legislation (or their closest equivalent concept or term as defined under such legislation).

2. ROLES AND SCOPE OF PROCESSING

- 2.1 Each party will comply with all applicable requirements of the Data Protection Legislation. This DPA is in addition to, and does not relieve, remove, or replace either party’s obligations under the Data Protection Legislation.
- 2.2 Where Supplier Processes Personal Data under this DPA, the Parties acknowledge that OT is either the Controller or, when Processing Personal Data under the instruction of a customer, a Processor, and the Supplier is therefore deemed to be either a Processor or Sub-processor to OT. If Supplier determines the purposes and means of any Processing of OT’s Personal Data Supplier shall become the Controller for such Processing and shall, consequently, be solely responsible for the lawfulness of such Processing by Supplier as Controller under applicable Data Protection Legislation. For the avoidance of doubt, Supplier is only permitted to Process Personal Data for the Business Purposes set out in clause 3.1.1 below.
- 2.3 Appendix A sets out details of the subject matter, nature and purpose of processing, type of personal data and categories of data subject. The duration of processing is the duration of the Agreement.

3. SUPPLIER’S OBLIGATIONS

General

- 3.1 To the extent that Supplier currently has, has had or will have access or potential access to Personal Data of OT and/or its customers, partner, employees, contractors or has or will generate, process, store or transmit

Personal Data in providing the Services, in relation to any Personal Data processed under the Agreement and this DPA, Supplier agrees to:

- 3.1.1 process, use and maintain Personal Data for OT and/or its customers only in accordance with OT's documented written instructions and the Agreement (together with this DPA) solely for the purposes of performing its responsibilities and obligations under the Agreement unless required to do so by applicable law as set out by Data Protection Legislation, provided that the Supplier shall notify OT of that legal requirement before Processing. The Supplier shall make no other use of Personal Data other than for the provision of the Services to OT. Supplier represents and warrants that nothing would prevent it from fulfilling such obligations.
- 3.1.2 keep up to date all Personal Data created or collected by Supplier directly from Data subjects on behalf of OT accurate and to delete or correct any inaccurate or incomplete Personal Data in accordance with OT's instructions.
- 3.1.3 where in the opinion of Supplier an instruction from OT infringes Data Protection Legislation, it shall inform OT thereof (but such communication shall not constitute legal advice by Supplier). However, such obligation shall not relieve Supplier from its own responsibility for compliance with Data Protection Legislation.
- 3.1.4 not Sell or Share the Personal Data.
- 3.1.5 not (a) Share or otherwise disclose the Personal Data to any third party except in accordance with the terms of this DPA for the purposes of the performance of the Services; (b) unless otherwise permitted by the Data Protection Legislation or this DPA for the purpose of performing the Services, combine Personal Data with other personal information it (i) receives from or on behalf of another person or third party, or (ii) collects from its own interactions with the applicable individual, (c) retain, use, disclose or otherwise Process the Personal Data outside of the direct business relationship between the Parties. Supplier certifies that it understands and will comply with all restrictions placed on its Processing of the Personal Data.

Security

- 3.2 Supplier shall take appropriate technical and organizational measures to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access or use, and against all other unlawful forms of Processing. Supplier agrees to comply with the terms of Appendix B: 'Technical and Operational Measures', which form part of this DPA, including the use of industry-recognized security standards such as ISO 27001 or similar standards where appropriate. The Supplier shall notify OT without undue delay in case of any changes to the technical and organizational matters which affect the Personal Data or that would otherwise reduce the level of protection of Personal Data.

Background Checks

3.3 Supplier shall ensure that only personnel who need to have access to Personal Data for provision of the Services are granted access to such Personal Data and only for the purposes of the performance of the Services; inform all personnel of the confidential nature of the Personal Data, and ensure personnel are subject to appropriate obligations of confidentiality and have received appropriate training on their responsibilities. In addition, Supplier shall carry out the following background verification checks:

For Supplier personnel in the United States:

- SSN Trace
- 7 Year County Criminal Report
- 7 Year Statewide Criminal Report
- 7 Year Federal Criminal Report
- Basic Employment Verifications (all employment within 7 years or most recent three employers)
- Education Verification (highest degree earned)
- Multi-state / Multi Jurisdiction Criminal Search
- Status on the Office of Foreign Assets Control (OFAC) list

For Supplier personnel outside the United States:

- SSN or (or SSN equivalent) Trace (inapplicable if jurisdiction does not have an SSN equivalent)
- International Criminal Search (checking all locations listed on candidate profile)
- International Employment Verifications (checking all employment within past seven years or most recent three employers)
- Education Verification (checking highest degree earned)

Cooperation

3.4 Supplier shall provide reasonable co-operation and assistance to OT (and the relevant Supervisory Authority, if applicable) in relation to compliance with OT's (and its customers) obligations under Data Protection Legislation including, but not limited to, in relation to: (i) any complaint or request made in respect of any Personal Data by any Data Subject including, but not limited to, assistance in responding to requests for exercising the Data Subject's rights of: access, rectification, erasure and objection, restriction of processing, data portability, and not to be subject to a decision based solely on automated processing; (ii) in the event of litigation or a regulatory inquiry concerning the Personal Data; and (iii) the carrying out of data protection impact assessments and/or consultations with a Supervisory Authority, all such cooperation and assistance to be provided at no additional charge and the Supplier will abide by the advice of OT and the relevant Supervisory Authority with regard to the Processing of Personal Data.

3.5 Where a Data Subject submits a request to the Supplier to exercise their rights, the Supplier shall forward these requests by email to OT at DPO@opentext.com or such other contact details expressly and directly notified by OT to Supplier in writing from time to time. The Supplier shall not respond to a Data Subject request unless and to the extent instructed by OT to do so.

3.6 Supplier shall inform OT without undue delay of any enquiry, complaint, notice or other communication it receives from any Data Protection Authority or any third party or governmental authority in connection with the Services provided by Supplier to DPO@opentext.com, unless prohibited from doing so by applicable law or competent court order.

4. BREACH NOTIFICATION

4.1 The Supplier shall without undue delay (but in any case within 24 hours) notify OT in writing (and by email at SED@opentext.com) if it becomes aware of (i) any Security Incident (ii) any accidental or unauthorized access to Personal Data, (iii) any actual or potential Personal Data Breach or breach of this DPA and / or Data Protection Legislation

4.2 Supplier shall without undue delay (but in any case within 24 hours) notify OT in writing (and by email at DPO@opentext.com) of (i) any disclosure or request for disclosure of Personal Data to a third party (except for disclosure to an approved Sub-processor in accordance with Clause 5.1) and (ii) any request for disclosure or inquiry from a third party (including, without limitation, a public authority) concerning the Personal Data unless such notification is prohibited by law; (iii) any change in applicable law that would render Supplier unable to comply with this DPA; (iv) Supplier makes a determination that it can no longer meet its obligations under this DPA or the Data Protection Legislation.

4.3 OT may take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Data, and Supplier shall cooperate with such efforts in addition to providing the notification set forth above.

4.4 If available and taking into account the nature of the Processing, the notification in accordance with clause 4.2 (i) and/or (ii) above shall at least:

- describe the nature of the Personal Data Breach including without limitation and where possible, the categories and approximate number of Data Subjects concerned, and the categories and approximate number of Personal Data records concerned.
- communicate the name and contact details of the data protection officer or other contact point where more information can be obtained.
- describe the likely consequences of the Personal Data Breach; and
- describe the measures taken or proposed to be taken by the Supplier to address the Personal Data Breach, including without limitation, where appropriate, measures to mitigate its possible adverse effects.

4.5 Where, and in so far as, it is not possible to provide the information at the same time or becomes available later, the information may be provided in phases without undue further delay.

5. SUB-PROCESSING

- 5.1 Supplier shall not subcontract any of its Processing operations performed on behalf of OT or any OT Affiliate to a new or replacement Sub-processor without the prior written consent of OT. The Supplier shall submit the request (by email to OT at subprocessor-change-notification@opentext.com) for prior written consent at least 60 days prior to the engagement of the sub-processor, together with the information necessary to enable OT to decide whether to provide its prior written consent. OT has provided consent to those Sub-processors set out at Appendix C. Where Supplier subcontracts its obligations, it shall do so only by way of a written agreement with the Sub-processor which imposes the same obligations on the Sub-processor as are imposed on Supplier under this DPA.
- 5.2 Supplier confirms that it has incorporated terms with its Sub-processors that are at least as restrictive as those set out in this DPA. Supplier will evaluate the security, privacy and confidentiality practices of a sub-processor prior to selection and on a regular basis to establish that it is capable of providing the level of protection of Personal Data required by this DPA. Supplier shall allow OT (or any Controller of the Personal Data, including OT customers, when applicable) to audit Sub-processors, and shall reasonably provide copies of relevant sub-processing clauses where required to do so as part of an audit, which might be redacted as appropriate by the Supplier. Where necessary to protect business secrets or other confidential information, including Personal Data. Supplier shall remain fully liable to OT for all acts and/or omissions performed by its Sub-processors.
- 5.3 Supplier shall not make a transfer of Personal Data (including, without limitation any Restricted Transfer of Personal Data by the Supplier to any Sub-processor), and procure that Sub-processors do not make a transfer of Personal Data, without the prior written consent of OT and provided always that such transfer and/or Restricted Transfer is compliant with Data Protection Legislation including, without limitation Standard Contractual Clauses entered into between the Supplier and relevant Sub-processor. The Supplier confirms that it has entered into Standard Contractual Clauses and/or Other Standard Contractual Clauses with all Sub-processors where there is a Restricted Transfer. Supplier shall provide copies of the applicable Transfer Mechanism in place with Sub-processors promptly if requested by OT (provided that Supplier may redact commercially sensitive and confidential information).
- 5.4 Supplier shall share all details relating to the new Sub-processor including any used Transfer Mechanism, the full details as prescribed under Appendix C and related Data Processing provisions with the said Sub-processor, upon request. OT will have the right to terminate the Agreement if the used Transfer Mechanism is invalidated and no alternative is put in place or when the related Data Processing provisions with the Sub-Processor are not or not adequately put in place.

6. AUDIT

- 6.1 For the purposes of this Section 6, references to OT includes to any Controller of the Personal Data, including OT customers, when applicable pursuant to Section 5.2.

6.2 Within five (5) business days of receipt of a written request from OT, the Supplier shall:

6.2.1 provide OT with reasonable access to its personnel, premises, facilities and Sub-processors to enable OT to conduct an on-site inspection audit;

6.2.2 provide evidence of Supplier's relevant policies and other related documents to verify that Supplier is complying with its obligations under this DPA; and

6.2.3 where available, provide a copy of the latest Service Organization Control (SOC) audit report and/or other third-party audit reports or information (in each case, provided by an entity reasonably acceptable to OT) to demonstrate the processing activities of Supplier relating to the Personal Data is in compliance with its obligations under this DPA.

6.3 Any on site audit under Clause 6.2.1 ("On Site Audit") shall be conducted during ordinary business hours on business days and shall not interfere unreasonably with Supplier's ordinary business. If the results of an On-Site Audit or other audit of information provided pursuant to Clause 6.2 (together an "Audit") show that Supplier is not complying with the Agreement and/or DPA, then Supplier must ensure prompt remedy of the non-compliance and comply with OT's reasonable directions to remedy the non-compliance, including without limitation directions as to timing. Any Audit shall be conducted, and all information to be provided pursuant to this clause shall be provided, at the cost of the Supplier.

7. DELETION OF OT DATA

Any Personal Data stored by the Supplier, or their Sub-processors shall be promptly returned to OT or OT customer upon the earliest of the following events: (i) upon OT request; or (ii) upon completion of all tasks for which the respective Personal Data was shared with the Supplier; or (iii) upon expiry or termination of Agreement. In the event that Personal Data cannot be returned, or if OT so elects, the Supplier shall destroy – and certify to OT in writing that it has destroyed – all such Personal Data within a time period considered reasonable under data protection or privacy laws (in any case not to exceed three months), unless a retention of the Personal Data is required or permitted by applicable law.

8. INDEMNIFICATION

The Supplier shall indemnify OT and its Affiliates from and against all claims, damages, expenses, losses or liabilities resulting from a breach of the DPA. Data Subjects may enforce the provisions of this DPA as a third-party beneficiary against Supplier with respect to their Personal Data. Breach of this DPA shall be deemed a material breach of the Agreement.

9. LIMITATION OF LIABILITY

Notwithstanding anything to the contrary agreed in the Agreement or elsewhere, the obligations of the Supplier under this DPA shall not be subject to any limitations or exclusions to the liability of the Supplier or its Affiliates.

10. GEOGRAPHICAL SPECIFIC DATA PROCESSING TERMS AND INTERNATIONAL TRANSFERS

The parties agree that Appendix D shall apply to supplement this Section 10 as it incorporates additional contractual terms required under Data Protection Legislation that apply in each of the jurisdictions set out in the referred Appendix. The parties agree to cooperate in good faith to negotiate amendments to such Appendix C where applicable under Data Protection Legislation.

Where the Data Protection Legislation provides for specific requirements for a Restricted Transfer to take place, the applicable Standard Contractual Clauses incorporated to this DPA under Appendix E shall apply.

11. CONFLICT

If there is an inconsistency between the terms in the Agreement and this DPA, such conflict will be resolved in the following order of precedence: (i) any terms and conditions in an SOW more restrictive than those included in this DPA; (ii) the Standard Contractual Clauses; (iii) this DPA; and (iv) the provisions of the Agreement in relation to the Processing of Personal Data, except for those included in subsection (i) of this paragraph.

12. OTHER PROVISIONS

12.1 The Parties agree that this DPA shall replace and supersede any existing data processing addendum, attachment, exhibit or standard contractual clauses that Supplier and OT may have previously entered into in connection with the Services. The parties confirm that in all other respects, the terms, covenants and conditions of the Agreement remain unchanged and in full force and effect, except as modified by this DPA. It is understood and agreed that all terms and expressions when used in this DPA, unless a contrary intention is expressed herein, have the same meaning as they have in the Agreement.

12.2 If the Supplier Processes Protected Health Information (“PHI”) as defined by HIPAA, Supplier shall execute a Business Associate agreement with OT and shall implement the applicable safeguards and processes for the handling of PHI that are specified in the HIPAA Privacy and Security Rules. Additionally, notwithstanding Section 12.1.1 above, any agreement or clauses entered into by the parties governing the processing of PHI in accordance with HIPAA will remain in effect for such purposes.

APPENDIX A

DETAILS OF THE PROCESSING OF PERSONAL DATA

Subject matter and duration of the Processing of Personal Data

Supplier is processing Personal Data in order to provide Services to OT and its affiliates under the Agreement

The duration of the Processing of the Personal Data is set out in the Agreement (and documentation governed by it) and this DPA.

The nature and purpose of the Processing of Personal Data

In the performance of Services under the Agreement, Supplier may from time to time perform data processing activities which may include, without limitation,

1. use of Personal Data to provide the Services.
2. collecting, recording, storing, structuring, modifying, adapting, altering or destroying the Personal Data of a Data Subject.
3. execution of instructions of OT in accordance with the Agreement and DPA.

The types of Personal Data to be processed

As further described in the Agreement, the categories of Personal Data may include without limitation the following:

1. Personal contact information (e.g. name, and personal addresses, phone numbers, and email addresses)
2. Work contact information (e.g. work addresses, phone numbers, and email addresses)
3. Detailed personal information (e.g. age and/or date of birth, gender, marital status, photos, former names, emergency contact information, and dependent information)
4. Identification number (e.g., employment number, social security number, social insurance number, driving license number, student number, national ID card number, and passport number)
5. Education and skills information (e.g. education history, degrees earned, institutions attended, academic records, qualifications, skills, training details, training records, professional expertise, work history and experience, and other resume/CV information)
6. Financial information (e.g. bank account information or details, information pertaining to salary, bonus, equity, taxes, benefits, credit, credit cards, and expenses)
7. Geo location / Time-zone
8. Any application-specific data
9. IT systems information (such as user credentials, computer name, domain name, IP address, and software usage pattern tracking information i.e. cookies)

Special categories of data (if appropriate)

As further described in the Agreement, the special categories of Personal Data within the scope of this DPA may include, without limitation sensitive personal data

The categories of Data Subject to whom the Customer Personal Data relates

Data subjects under this DPA may include, without limitation:

1. Employees and other staff members, agents, suppliers, advisors or sub-contractors of OT's end customer(s) and/or their client(s).
2. User's of OT's end Customer's software or application(s) or services;
3. Employees and other staff members, agents, suppliers, advisors or sub-contractors of OT or its Affiliates.
4. Partners of OT or of its Affiliates, including without limitation their employees and other staff members, agents, suppliers, advisors or sub-contractors
5. Any other natural person or individual having Personal Data stored, transmitted to, made available to, accessed or otherwise processed by Supplier.

APPENDIX B

TECHNICAL AND ORGANIZATIONAL MEASURES (IT SECURITY TERMS AND CONDITIONS)

Supplier must comply with the Technical and Organizational Measures (**IT Security Terms and Conditions**) including, without limitation, its appendices and ensure any subcontractor engaged by the Supplier, also complies with the Technical and Organizational Measures for any processing of OpenText Data.

For the Technical and Organizational Measures (**IT Security Terms and Conditions**) see [here](#) as may be amended, updated or replaced from time to time (which are also available on OpenText's Supplier Information page: <https://www.opentext.com/about/supplier-information>).

These Technical and Organizational Measures (IT Security Terms and Conditions) are incorporated into this DPA by reference (with the same force and effect as though fully set forth in this DPA).

References to OpenText information, OpenText data and OpenText assets shall be deemed to include Personal Data of OpenText and/or its customers or other Personal Data that Supplier has or will generate, process, store or transmit in providing the Services.

**APPENDIX C
SUB-PROCESSORS AND LOCATIONS OF PROCESSING**

In the event there is any international data transfer the Supplier will provide information relating to the jurisdictions the processing of Personal Data will take place and provide it in the format set out below.

Approved Sub-processors and locations of processing by those Sub-processors are set out below:

Supplier Group Sub-processors:

Name	Address	Contact person's name, position and contact details	Sub-processor location(s)	Locations of onward data transfers by Sub-processor	Description of the processing (including a clear delimitation of responsibilities in case several sub-processors are authorised)	Transfer Mechanism

Third Party Sub-processors

Name	Address	Contact person's name, position and contact details	Sub-processor location(s)	Locations of onward data transfers by Sub-processor	Description of the processing (including a clear delimitation of responsibilities in case several Sub-processors are authorised)	Transfer Mechanism

APPENDIX D

GEOGRAPHICAL SPECIFIC TERMS

USA: To the extent Supplier is Processing Personal Data that is subject to the California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act (“CCPA”) as a Processor under this DPA, the parties agree Supplier does so acting in the role of a Service Provider (as defined under CCPA).

APPENDIX E INCORPORATION OF TRANSFERS MECHANISMS

A- Transfers subject to Data Protection Legislation applicable in the European Economic Area (EEA)

The Parties hereby agree that Restricted Transfers subject to Data Protection Legislation applicable in European Economic Area jurisdictions shall be governed by the SCCs approved by the [COMMISSION IMPLEMENTING DECISION \(EU\) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation \(EU\) 2016/679 of the European Parliament and of the Council \(EEA SCCs\)](#), the mandatory clauses of which are incorporated into this Agreement by reference, and completed as agreed in this Section A of Schedule 3 (as set out in the table below), unless other Transfer Mechanism applies.

SCCs Clause	Module Two Controller to Processor	Module Three Processor to Processor
1	Incorporated	
2		
3		
4		
5		
6		
7		
8	General and Module Two provisions	General and Module Three provisions
9	For clause 9 (a) the Parties choose Option 2, agreeing on a period of 30 business days.	
10	General and Module Two provisions	General and Module Three provisions
11	In clause 11 (a) the optional clause shall be incorporated	
12	General and Module Two provisions	General and Module Three provisions
13	For paragraph 13 (a), the competent Supervisory Authority shall be the competent Supervisory Authority that has supervision over the relevant data exporter.	
14	General and Module Two provisions	General and Module Three provisions
15	The Parties select option 1, being the governing law the Data Protection Legislation (as defined in the Agreement) applicable to the data exporter	
16		
17		
18	General and Module Two provisions	General and Module Three provisions
	Regarding the choice of court and jurisdiction, the Parties choose the court where the data exporter is based.	
Appendices	Shall be completed as applicable with the details agreed in Appendices A, B, C and F of this DPA.	

B- Transfers subject to Data Protection Legislation applicable in Switzerland

Where a Restricted Transfer is subject to Swiss Data Protection Legislation, the EEA SCCs shall apply, amended as follows:

- a) References to the GDPR shall be understood as references to the Swiss Federal Act on Data Protection (as such laws are amended or re-enacted from time to time) (“**FADP**”);
- b) The “competent supervisory authority” is the Federal Data Protection and Information Commissioner;
- c) Where the transfer is subject to both the FADP and the GDPR (as defined in the EEA SCCs), the supervisory authority is the Swiss Federal Data Protection and Information Commissioner insofar as the transfer is governed by the FADP, and the supervisory authority is as set forth in the EEA Standard Contractual Clauses insofar as the transfer is governed by the GDPR;
- d) The term “personal data” shall be deemed to include the data of legal entities to the extent such data is protected under the FADP;
- e) Clause 18 (c) shall be interpreted to permit data subjects in Switzerland to bring legal proceedings in Switzerland.

C- Transfers subject to Data Protection Legislation applicable in the United Kingdom (UK)

Where a Restricted Transfer is subject to Data Protection Legislation of the United Kingdom the EEA SCCs incorporated to this Agreement shall apply, as amended under the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (a.k.a. EEA SCCs) issued by the Information Commissioner’s Office under S119A(1) Data Protection Act 2018 (version B1.0, in force 21 March 2022), a copy of which is available here [international-data-transfer-addendum.pdf](#) shall apply, and completed as follows:

Part 1 Table 1 “Parties” shall be completed as follows:

- Start Date shall be the “Effective Date of the Agreement”
- Exporters and Importers are as set out in Appendix G
- Key contacts shall be as set out in Appendix G.

Part 1 Table 2 “Selected SCCs, Modules and Selected Clauses”, the Parties choose “the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum” as the option for the “Addendum EU SCCs”, for which: Modules 2 and 3 are incorporated, of which: Optional clause 7 “Docking Clause” is incorporated; Clause 11 is excluded from all applicable Modules, Clause 9a of Modules 2 and 3 incorporated the General Authorisation option and notifications timeframe of 14 business days.

Part 1 Table 3 “Appendix Information” is completed with the details agreed in Appendices A, B, C and F of this DPA.

Part 1 For Table 4: “Ending this Addendum when the Approved Addendum Changes” the Parties choose that neither Party may end this Addendum as set out in Section 19 of these SCCs.

Part 2 Mandatory Clauses shall consist of the 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 5.3 of those Mandatory Clauses.

D- Transfers subject to Data Protection Legislation applicable in Turkey

Where a Restricted Transfer is subject to Data Protection Legislation applicable in Turkey, Modules 2 and 3 of the following Modules of the Standard Contract for the Transfer of Personal Data Abroad issued by the Data Protection Authority (KVKK), which are available here, [KİŞİSEL VERİLERİ KORUMA KURUMU | KVKK | Announcement on the Translation of By-Law on the Procedures and Principles for the Transfer of Personal Data Abroad and Standard Contract Texts](#) shall apply and completed as follows:

- The Parties choose to apply the General Authorization option provided in Clause 8 and provide a 14 business days period of time for notification concerning sub-processors.
- Clause 10 Redress shall exclude the optional provisions.
- The Party notifying the Authority according to Clause 16 shall be the Data Exporter.
- Data Exporters and Data Importers shall be those set out in Appendix G.
- Appendix 1 Annex I and Annex II shall be completed with the details set out in Appendices A, B, C and F of this DPA.
- The personal data transferred under the Turkish SCCs shall be subject to the retention periods as set out in the Agreement or the DPA.
- Appendix 1 Annex III “List of Sub-processors” shall be completed as agreed in Appendix C of this DPA.

E- Transfers subject to Data Protection Legislation applicable in China

Where a Restricted Transfer is subject to Data Protection Legislation applicable in China, the China standard contractual clauses Outbound Transfer of Personal Information (China SCCs) here available [个人信息出境标准合同办法 中央网络安全和信息化委员会办公室](#) are incorporated in the Agreement and completed as follows:

- The Personal Information Handler and the Overseas Recipient carry out activities of outbound transfer of the personal information are those detailed in the Agreement.
- For the purposes of Article 2 paragraph 5, the applicable technical and security measures are those attached to the DPA.
- For the purposes of Article 9 paragraph 3, notifications will be sent to the email addresses detailed in the DPA. If the notice under this Agreement is sent by registered airmail, it shall be deemed to have been received within 05 days after the postmark date; if it is sent by email, telegram, telex or fax, it shall be deemed to have been received within 03 working days after it is sent.
- For the purposes of Article 9 paragraph 3, disputes will be submitted to Other arbitral institutions in the jurisdictions that are members of the Convention on the Recognition and Enforcement of Foreign Arbitral Awards (The International Court of Arbitration (ICC) – UK Branch). And the arbitration shall be conducted in London (place of arbitration) in accordance with its arbitration rules then in force.
- Appendices I and II Shall be completed as applicable with the details agreed in Appendices A, B, C, and F of this DPA.

Supplier commits to process personal information in accordance with the terms of the China SCCs and not exceed the agreed scope of processing unless separate consent is obtained from the personal information subject (if applicable).

F- Transfers subject to Data Protection Legislation applicable in Saudi Arabia

Where a Restricted Transfer is subject to Data Protection Legislation applicable in Saudi Arabia, The Saudi Arabia standard contractual clauses for the Modules Controller to Processor or Processor to Processor as the case may be (as approved by the Saudi Data and AI Authority (SDAIA) and published at [StandardContractualClausesForPersonalDataTransferEN.pdf](#) (SA SCC)) apply and be completed as follows:

- Information required to complete the Appendices 1 to 3 of the SA SCC can be found in Appendices A, B, C, and F of this DPA.

G- Incorporation of New Standard Contractual Clauses

Where competent authorities issue New Standard Contractual Clauses that are deemed to apply in the context of the Data Processing Activities agreed in this DPA, either in addition to the already incorporated SCCs or under a mandatory requirement to replace these, the New SCCs shall directly apply, or where appropriate, directly replace the concerned SCCs and be deemed to take effect and form a binding contract between the parties detailed in Appendix G of this DPA, from the date on which the New SCCs becomes legally mandatory, enforceable and applicable to allow for a Restricted Transfer.

Where not otherwise expressly incorporated into this Agreement, the New SCCs shall be competed as follows:

- Appendices A, B, C, and F of this DPA shall be incorporated into the new SCCs.
- Any optional clauses shall be excluded, unless otherwise expressly agreed in writing in a clause incorporated to this DPA.
- Where an option to choose an express or general authorization, applicable to any clauses, the general authorization shall apply.
- Periods to notify Parties, for which the Parties have an option to choose, shall be of 14 business days in general, and 48 hours for Personal Data Breaches.
- Where rights conceded to Parties are subject to selection between exporter, importer, or none of them, the option selected shall be “none of them”, if not available, the exporter shall be selected.
- The designated Data Protection Authority shall be the authority overseeing and/or enforcing the Data Protection Legislation applicable in the country in which the exporter is based.
- Where an obligation to register or notify the designated Data Protection Authority must be allocated to either the exporter or the importer, the party chosen shall be the exporter.
- The applicable law and jurisdiction chosen shall be those applicable in the location where the exporter is based.

G- Hierarchy applied to incorporated Transfer Mechanisms

In the event of coexistence or contradiction between Transfer Mechanisms incorporated into this DPA, the following prevalence order shall apply:

- 1- Derogations, where and to the extent that apply to OT.
- 2- Other Transfer Mechanisms to which OT is adhered to or being granted with.
- 3- Standard Contractual Clauses that have been expressly incorporated into this DPA.
- 4- New Standard Contractual Clauses.

APPENDIX F

INTERNATIONAL DATA EXPORT REQUIREMENTS

The Supplier certifies and confirms that the responses provided by the Supplier in the Privacy and IT Security Questionnaire are true and accurate in respect of both the Supplier and its Sub-processors and that the Supplier and its Sub-processors are compliant with such responses. The Supplier shall notify OT promptly of any actual or potential change that would impact the responses provided.

Supplier will adopt supplementary measures to provide such safeguards for the Personal Data as are necessary, in particular as regards to any access by public authorities, to protect the Personal Data against any interference that goes beyond what is necessary and proportionate in a democratic society to safeguard national security, defence and public security and/or that would impinge on the parties' ability to comply with the Standard Contractual Clauses.

The Supplier commits to provide evidence of supplementary measures that ensure the protection of the Personal Data.

APPENDIX G
TRANSFER SIGNATORY PARTIES

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

Name:	OT (as defined in the DPA)
Address:	As set out in the Agreement.
Contact person's name, position and contact details:	DPO@opentext.com OT Data Protection Officer Prof. E.M. Meijerslaan 1 1183 AV Amstelveen The Netherlands
Activities relevant to the data transferred under these Clauses: OT is obtaining Services from the Supplier.	
Role:	Controller or Processor (as applicable)

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

Name:	Supplier (as defined in the DPA)
Address:	As set out in the Agreement.
Contact person's name, position and contact details:	Contact details as set out in the Agreement
Activities relevant to the data transferred under these Clauses: Provision of Services pursuant to the Agreement.	
Role:	Processor or Sub-processor