opentext™

Open Text Data Processing Addendum

Parties

This Data Processing Addendum ("DPA") is between:

A. The Open Text entity ("OT") having entered into the Principal Agreement (as defined below) acting on its own behalf; and

B. the other party to the Principal Agreement ("Customer").

OT and Customer hereinafter separately referred to as "Party" and jointly as "Parties".

1. Background; Definitions.

1.1 Background.

1.1.1 This DPA (including its Appendices and incorporations by reference) supplements and forms part of the agreement between OT and Customer under which OT shall carry out certain Services ("Principal Agreement") provided that the Services include the Processing of Personal Data and Data Protection Legislation applies to Customer's use of the Services.

1.1.2 This DPA is in addition to, and does not relieve, remove, or replace either party's obligations under the Data Protection Legislation.

1.1.3 None of the terms and conditions of the Principal Agreement shall be waived or modified by this DPA but if there is any conflict between any of the provisions of this DPA and the provisions of the Principal Agreement in relation to the Processing of Personal Data, the Parties agree the provisions of this DPA shall prevail to the extent of any such conflict.

1.1.4 If there is any conflict between the provisions of this DPA and the provisions of the Standard Contractual Clauses, the provisions of the Standard Contractual Clauses shall prevail to the extent of any such conflict. For the avoidance of doubt, where this DPA further specifies Sub-processor and audit rules in Sections 2.3 and 2.11, such specifications also apply in relation to, and satisfy Customer rights under the respective provisions of the Standard Contractual Clauses.

1.1.5 The terms used in this DPA shall have the meanings set forth in this DPA. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement.

1.2 Definitions.

1.2.1 In this DPA, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly.

A. "Affiliate" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with a company, 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.

B. "Data Protection Legislation" means, (i) the GDPR (and any laws of Member States of the European Economic Area ("EEA") implementing or supplementing the GDPR), (ii) UK Data Protection Law and (iii) data protection or privacy laws of Switzerland, in each case, to extent applicable to the Processing of Personal Data under this DPA and the Principal Agreement.

C. "EEA Standard Contractual Clauses" means the EEA Controller to Processor SCCs and EEA Processor to Processor SCCs.

D. "EEA Controller to Processor SCCs" means the clauses set out as Appendix 4, as may be amended, updated or replaced from time to time.

E. “EEA Processor to Processor SCCs” means the clauses set out Appendix 5, as may be amended, updated or replaced from time to time.

F. “GDPR” means EU General Data Protection Regulation 2016/679.

G. “Restricted Transfer” means a transfer of Personal Data which, subject to the paragraph below, is:

(1) from an exporter subject to GDPR which is only permitted in accordance with GDPR if a Transfer Mechanism is applicable to that transfer (“EEA Restricted Transfer”);

(2) from an exporter subject to UK Data Protection Law which is only permitted in accordance with UK Data Protection Law if a Transfer Mechanism is applicable to that transfer (“UK Restricted Transfer”); and/or

(3) from an exporter subject to Data Protection Legislation applicable in Switzerland which is only permitted under that law if a Transfer Mechanism is applicable to that transfer (“Swiss Restricted Transfer”).

Transfers of Personal Data will not be considered a Restricted Transfer where:

(a) the jurisdiction to which the personal data is transferred has been approved by the European Commission under Article 45 of the GDPR or, as applicable, an equivalent provision under UK or Swiss Data Protection Law, as ensuring an adequate level of protection for the processing of Personal Data (an “Adequate Country"); or

(b) the transfer falls within the terms of a derogation as set out in Article 49 of the GDPR, equivalent under Swiss Data Protection Law or the UK GDPR (as applicable).

H. “Services” means the services or products and other activities to be supplied to or carried out by or on behalf of OT for the Customer pursuant to the Principal Agreement.

I. “Standard Contractual Clauses” means each of the EEA Standard Contractual Clauses and the UK Standard Contractual Clauses.

J. “Sub-processor” means any third party (including any OT Affiliate) appointed by or on behalf of OT as a sub-contractor to Process Personal Data on behalf of any Customer or Customer Affiliate in connection with the Principal Agreement.

K. “Technical and Organisational Measures” means the technical and organisational measures set out as Appendix 3, as may be amended, updated or replaced from time to time.

L. “Transfer Mechanism” means the Standard Contractual Clauses or any other appropriate safeguards under article 46 of the GDPR or equivalent under Swiss or UK Data Protection Law applicable to a relevant transfer of Personal Data that has the effect of permitting that transfer.

M. “UK Data Protection Law” means UK GDPR (as defined in the UK Data Protection Act 2018) and the UK Data Protection Act 2018.

N. “UK Controller to Processor SCCs” means the UK International Data Transfer Addendum which is made up of the provisions set out as Appendix 6, as may be amended, updated or replaced from time to time, and incorporating the EEA Controller to Processor SCCs.

O. “UK Processor to Processor SCCs” means the UK International Data Transfer Addendum which is made up of the provisions set out as Appendix 6, as may be amended, updated or replaced from time to time, and incorporating the EEA Processor to Processor SCCs.

P. “UK Standard Contractual Clauses” means the UK Controller to Processor SCCs and UK Processor to Processor SCCs.

1.2.2 The terms “Controller”, “Data Subject", “Personal Data", “Personal Data Breach", “Processing", and “Processor”; shall have the same meaning as in the applicable Data Protection Legislation. The terms “Member State", “Supervisory Authority” and “Union” shall have the same meaning as in the GDPR. The terms “data

exporter" and "data importer" have the meaning set out in the applicable Standard Contractual Clauses. "including" shall mean including without limitation.

2. Data Processing Obligations.

2.1 Controller and Processor of Personal Data, Appointment of Processor and Purpose of Processing.

2.1.1 OT will comply with all applicable requirements of the Data Protection Legislation to the extent it imposes obligations upon OT as a Data Processor and expects Customer to also comply with Data Protection Legislation.

2.1.2 This DPA applies to the extent Customer is the Controller and OT is the Processor. It also applies to the extent that Customer is a Processor and OT is acting as a (sub) Processor. Where the Customer is a Processor, the Customer confirms that its instructions, including appointment of OT as a Processor or (sub) Processor, have been authorized by the relevant Controller.

2.1.3 Appendix 1 of this DPA sets out the scope, nature and purpose of Processing by OT, the duration of the Processing and the types of Personal Data and categories of Data Subjects.

2.2 OT's obligations with respect to the Customer.

2.2.1 OT will, in relation to any Personal Data it will be Processing under the Principal Agreement and this DPA:

A. process such Personal Data solely for the purpose of providing the Services;

B. process such Personal Data in accordance with documented and commercially reasonable instructions from the Customer, subject to and in accordance with the terms of the Principal Agreement;

C. ensure that the persons authorized by it to process such Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and have received appropriate training on their responsibilities; and

D. limit access of OT personnel to the Personal Data undergoing processing to what is necessary for provision of the Services.

2.2.2 Customer agrees that the Principal Agreement (including this DPA) are its complete documented instructions to OT for the Processing of Personal Data. Additional instructions, if any, require prior written agreement between the Parties. Where in the opinion of OT an instruction from the Customer infringes Data Protection Legislation, it shall inform the Customer thereof (but such communication shall not constitute legal advice by OT). However, such obligation shall not relieve the Customer from its own responsibility for compliance with Data Protection Legislation.

2.2.3 Where OT is required under applicable law to process Personal Data other than on documented instructions from the Customer, including with regard to transfers of Personal Data to a third country or an international organisation, OT shall use its reasonable endeavours to inform the Customer of that legal requirement before Processing, unless such information is prohibited by law on important grounds of public interest.

2.3 Sub-processing.

2.3.1 Customer provides OT a general authorization to engage Sub-processors. Sub-processors may include: (i) OT's global Affiliate companies as exist from time to time (and their vendors); and/or (ii) any of the sub-contractors that OT engages in connection with the provision of certain Processing activities as at the date of this Agreement. The Parties agree that the sub-processors listed at (i) and (ii) is the 'agreed list' for sub-processors in relation to Clause 9(a) of the EEA Standard Contractual Clauses and for the UK Standard Contractual Clauses.

2.3.2 OT shall Inform the Customer at least 14 days before OT appoints a new or replacement Sub-processor to give the Customer opportunity to reasonably object to the changes. OT must receive the notice of objection in writing from the Customer within 14 days of OT informing it of the proposed changes. The Parties agree that the name of the new or replacement Sub-processor together with details of the processing activities it will carry out and the location of such activities is the information the Customer requires to exercise such right. "Inform" shall include by posting the update on a website (and providing Customer with a mechanism to obtain notice of

that update), by email or in other written form. The parties confirm that this mechanism is not required where the new or replacement Sub-processor is an OT global Affiliate company.

2.3.3 The Parties agree that the Customer's right to be object shall be as set out in this Section 2.3.3 and Section 2.3.4. Any objection raised by the Customer pursuant to Section 2.3.2 must be where the Sub-processor demonstrably fails to offer the same or a reasonably comparable level of protection as that previously applicable to the relevant Processing of Personal Data.

2.3.4 If Customer has a reasonable and legitimate reason to object to the new Sub-processor pursuant to Section 2.3.3, and OT is not able to provide an alternative Sub-processor, or the Parties are not otherwise able in good faith to achieve an alternative resolution, Customer may terminate the respective part of the Services where the new Sub-processor is to be used by giving written notice to OT no later than 30 days from the date that OT receives the Customer's notice of objection and such termination shall take effect no later than 90 days following OT's receipt of Customer's notice of termination. If Customer does not terminate within this 30-day period, Customer is deemed to have accepted the new Sub-processor. Any termination under this Section 2.3.4 shall be deemed to be without fault by either Party and shall be subject to the terms of the Principal Agreement (including any documents agreed pursuant to it).

2.3.5 OT confirms that it has entered or (as the case may be) will enter into a written agreement with its third-party company Sub-processors incorporating terms which are substantially similar to those set out in this DPA.

2.3.6 As between the Customer and OT, OT shall remain fully liable for all acts or omissions of any Sub-processor appointed by it pursuant to this Section 2.3 (unless the Sub-processor acted in accordance with instructions directly or indirectly received from Customer).

2.4 Data Subjects' Right to Information. It is the Customer's (or the party acting as Controller) responsibility to inform the Data Subject(s) concerned of the purposes and the legal basis for which their Personal Data will be processed at the time the Personal Data is collected.

2.5 Exercise of Data Subjects' Rights.

2.5.1 Taking into account the nature of the Processing, OT shall assist the Customer insofar as this is possible and reasonable for the fulfilment of the Customer's obligation under Data Protection Legislation to respond to requests for exercising the Data Subject's rights of: access, rectification, erasure and objection, restriction of processing, data portability, not to be subject to a decision based solely on automated processing.

2.5.2 Where the Data Subjects submit requests to OT to exercise their rights, OT shall forward these requests by email to a Customer email address on file with OT. If Customer wishes for OT to forward Data Subject requests to a specific email address, it shall notify OT of such address. OT shall not respond to a Data Subject request unless and to the extent instructed by Customer to do so.

2.6 Notification of Personal Data Breach.

2.6.1 OT shall notify the Customer of a Personal Data Breach without undue delay after OT becoming aware of it by email to a Customer email address on file with OT, along with any necessary documentation to enable the Customer, where necessary, to notify this breach to the Data Subject and / or the competent Supervisory Authority.

2.6.2 If available and taking into account the nature of the Processing, the notification in accordance with Section 2.6.2 shall at least:

A. describe the nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects concerned, and the categories and approximate number of Personal Data records concerned;

B. communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

C. describe the likely consequences of the Personal Data Breach; and

D. describe the measures taken or proposed to be taken by OT to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

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

2.6.4 The Customer (or the party acting as Controller) is responsible to notify the Personal Data Breach to the Supervisory Authority, and to the Data Subjects, when this is required by the applicable Data Protection Legislation.

2.7 Assistance lent by OT to the Customer regarding Compliance with Customer's Obligations under the Data Protection Legislation.

2.7.1 Where requested by the Customer and to the extent required by Data Protection Legislation, OT shall, taking into account the nature of processing and the information available to OT, provide reasonable assistance to the Customer:

A. in carrying out data protection impact assessments; or

B. should the Customer need prior consultation with a Supervisory Authority.

2.8 Security Measures.

2.8.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Customer and OT shall both be responsible to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

2.8.2 OT agrees to implement the Technical and Organizational Measures in respect of the Services.

2.8.3 Customer is responsible for implementing and maintaining privacy protections and security measures for components that Customer or any Customer Affiliate provides or controls. Customer shall apply the principle of data minimisation and limit OT access to systems or Personal Data to only where essential for the performance of Services. Where OT is performing Services on premises of the Customer (or of any Customer Affiliate or sub-contractor, agent or similar) or in connection with access to any of their systems and data, Customer shall be responsible for providing OT personnel with user authorizations and passwords to access those systems, overseeing their use of those passwords and terminating these as required. Customer shall not store any Personal Data in a non-production environment unless it has production environment equivalent controls in place.

2.9 Data Return or Destruction. Where OT has stored Personal Data as part of the Services: at the end of the Service(s) upon Customer's written instruction, OT may (i) offer a data return service or (ii) following a reasonable data retention period delete the Personal Data unless applicable law requires further storage of the Personal Data. OT may charge a fee for any data return services.

2.10 The Data Protection Officer. OT has designated a data protection officer in accordance with Data Protection Legislation. They can be contacted by email via DPO@opentext.com.

2.11 Inspections and Audits.

2.11.1 The right of audit, including inspections, which the Customer may have under Data Protection Legislation and under the Standard Contractual Clauses, are as set out in this Section 2.11.

2.11.2 Upon written request from Customer OT shall, where available, provide a copy of the latest Service Organization Control (SOC) audit report and/or other third-party audit reports or information to demonstrate the processing activities of OT relating to the Personal Data is in compliance with its obligations under this DPA.

2.11.3 Customer may request evidence of OT's relevant policies and other related documents to verify that OT is complying with its obligations under this DPA.

2.11.4 Customer may conduct an on-site inspection at OT's premise either by itself or by an independent third-party auditor (not to include a competitor of OT) where the information under Sections 2.11.2 and 2.11.3 has failed to verify compliance by OT of its obligations under this DPA or such an inspection is formally required by the Supervisory Authority.

2.11.5 General Procedure: The following Sections 2.11.6, 2.11.7 and 2.11.8 shall apply to each of Sections 2.11.2, 2.11.3 and 2.11.4.

2.11.6 Unless otherwise mandated by a Supervisory Authority, Customer shall: (a) give OT at least 30 days' prior written notice of its intention to conduct an audit, including inspection, under this Section 2.11; and (b) agree with OT the frequency and duration of these, which shall not extend beyond two consecutive business days nor be more than once per contract year.

2.11.7 Any audit, including inspections, must be conducted during local business hours, not unreasonably disrupt OT business operations and not burden the provision of services by OT to its customers. Customer shall limit these to remote audits or meetings with senior representatives of OT as far as possible and will avoid or minimise the need for an audit (including inspection), without limitation by using current certifications, other audit reports or combining them with others under the Principal Agreement. Additionally, these rights are subject to limitations set out in the Principal Agreement. Any audit, including inspections, shall be subject to OT's relevant policies and procedures.

2.11.8 Conditions of confidentiality and the scope of an audit, including inspection, shall be agreed in advance between OT and Customer. Customer shall provide OT the results of any audit, including inspection. Customer bears all expenses related to inspections and audits.

2.12 Customer Information and related Restrictions.

2.12.1 Instructions by Customer related to the Processing of Personal Data must be provided in writing duly signed by an authorised representative of Customer.

2.12.2 Customer is responsible to have all necessary consents and notices in place and confirms it is entitled to lawfully transfer the Personal Data to OT.

3. International Transfers.

3.1 Personal Data may be processed in the EEA, the United Kingdom and Switzerland (each a "Designated Country") and in countries outside of a Designated Country ("Other Countries") by OT or its Sub-processors. The transfer to Other Countries shall be in accordance with Data Protection Legislation (to the extent it applies).

3.2 The Parties shall have in place a Transfer Mechanism in respect of any Restricted Transfer:

3.2.1 In the event of an EEA Restricted Transfer where Personal Data is transferred from Customer as data exporter acting as a Controller or Processor (as applicable), to OT as data importer acting as a Processor, the Parties shall, as part of this DPA, comply with the EEA Controller to Processor SCCs where the Customer acts as a Controller and the EEA Processor to Processor SCCs where the Customer acts as a Processor.

3.2.2 In the event of a UK Restricted Transfer, where Personal Data is transferred from Customer as data exporter acting as a Controller or Processor (as applicable) to OT as data importer acting as a Processor, the Parties shall, as part of this DPA, comply with the UK Controller to Processor SCCs where the Customer acts as a Controller and the UK Processor to Processor SCCs where the Customer acts as a Processor.

3.2.3 In the event of a Swiss Restricted Transfer, whereby Personal Data is transferred from Customer as data exporter, acting as a Controller or Processor (as applicable), to OpenText as data importer acting as a Processor, the Parties shall, as part of this DPA, comply with the corresponding module of the EEA Standard Contractual Clauses.

3.2.4 The Standard Contractual Clauses will not apply to a Restricted Transfer to the extent that OT has adopted Binding Corporate Rules for Processors or an alternative recognised compliance standard for lawful Restricted Transfers.

3.3 Where pursuant to the Standard Contractual Clauses OT attempts to redirect a request from a public authority, including judicial authorities ("Government Request") to the Customer, and/or determines that a requirement to challenge or appeal a Government Request regarding Customer's Personal Data exists, Customer agrees to participate in and support such challenge as reasonably requested. Where possible, the Customer itself will seek a protective order or other appropriate remedy in response to the Government Request.

4. General Provisions.

4.1 Execution of this DPA. Where requested by Customer, OT and Customer shall execute this DPA in one or more counterparts, each of which shall be deemed an original and all of which together shall constitute one and the same instrument. For the purposes hereof, a facsimile or scanned copy of this DPA, including all pages hereof, shall be deemed an original.

4.2 The Parties agree that with respect to the period on and after the date that this DPA comes into effect between the Parties (or if earlier, the mandatory date when the relevant Standard Contractual Clauses must apply), this DPA shall replace and supersede any existing data processing addendum, attachment, exhibit or standard contractual clauses that Customer and OT may have previously entered into in connection with the Services.

5. For Partner Agreements.

5.1 If the Principal Agreement relates to the resale or supply of Services with a partner under an OT partner programme or a partner agreement (a "Partner"), with OT acting as the Partner's sub-processor under that arrangement with no direct contractual relationship to the direct and indirect customers of the Partner which are entitled to use the Services such as the End User or, in the case of a Partner who is an MSP, the Beneficiary (as in each case as defined in the Principal Agreement) (hereinafter "Using Parties"), then the following provisions shall apply:

5.1.1 All references to "Customer" in this DPA shall mean the Partner;

5.1.2 Section 2.8.3 of this DPA shall be amended to read as follows: "Partner shall procure implementation and maintenance of privacy protections and security measures for components that Partner or any Using Parties (including Affiliates of any of these) provides or controls. Partner shall apply the principle of data minimisation and limit OT access to systems or Personal Data to only where essential for the performance of Services (and procure the same from Using Parties). Where OT is performing Services on premises of the Partner or Using Parties (or of an Affiliate, sub-contractor, agent or similar of any of these) or in connection with access to any of their systems and data, Partner shall be responsible for procuring provision to OT personnel of user authorizations and passwords to access those systems, oversight of their use of those passwords and termination of these as required. Partner shall not store any Personal Data in a non-production environment unless it has production environment equivalent controls in place (and procure the same from Using Parties)."

APPENDIX 1
DETAILS OF PROCESSING OF CUSTOMER PERSONAL DATA

See Appendix 2 of this DPA for each of following: *Subject matter and duration of the Processing of Personal Data, the nature and purpose of the Processing of Personal Data, the types of Personal Data to be processed, special categories of data (if appropriate) and the categories of Data Subject to whom the Customer Personal Data relates.*

APPENDIX 2
DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred
Data Subjects may include employees, contractors, business partners or other individuals having Personal Data stored, transmitted to, made available to, accessed or otherwise processed by OT.

Categories of personal data transferred
Customer determines the categories of Personal Data which are processed by OT in connection with the Services in accordance with the terms of the Principal Agreement (and documentation governed by it). Customer submits Personal Data for processing after careful evaluation of compliance with applicable laws. The Personal Data may include the following categories of data: name, phone numbers, e-mail address, time zone, address data, company name, plus any application-specific data.
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.
None.
The choice and type of Personal Data that will be processed using the OT Services remains solely within the discretion and choice of the Customer. In selecting the Personal Data of any categories, the Customer shall ensure that such Personal Data is suitable for processing with and through the Services in compliance with applicable data protection laws. OT disclaims all liabilities in relation to the selection of data for use with the Services.

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

Nature of the processing
OT offers its Services, and in doing so, OT requires to process Personal Data.
The Personal Data is subject to the basic processing activities as set out in the Principal Agreement which may include:
(a) use of Personal Data to provide the Services;
(b) storage of Personal Data;
(c) computer processing of Personal Data for data transmission; and
(d) other processing activities to deliver the Services.

Purpose(s) of the data transfer and further processing
See “nature of processing” above.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
The duration of the Processing of the Personal Data is set out in the Principal Agreement (and documentation governed by it) and this DPA.

Subject matter, nature and duration of the processing for transfer to (sub-) processors
As above.

OT partner programs and partner agreements: Where section 5 of the DPA applies: for the purposes of these Appendices 1, 2 and 3, categories of Personal Data shall also include that of Using Parties (as defined in section 5 of the DPA). In Appendix 3, “Customer systems” refers to those of the Partner and Using Parties. Notwithstanding the foregoing, this shall not release the Partner of its obligations, either in these Appendices, the Annexes, the DPA or otherwise, and the Partner shall remain responsible for the decisions, acts and omissions of Using Parties, and shall procure that Using Parties comply with the provisions of these Appendices.

APPENDIX 3
Technical and Organizational Measures

This Appendix 3 describes the technical and organisational security measures used by Open Text to the extent that it is a Processor, and where in such capacity it (a) hosts or stores Customer Personal Data on its servers or systems or (b) it has access to Customer systems containing Personal Data.
Open Text may implement changes to these measures at any time without notice. provided such changes do not result in a material degradation of the overall level of security for Personal Data.

Physical Access Control

This control describes the measures to regulate access to Open Text data centres.

Data centre facilities are designed to physically protect equipment and other critical resources from unauthorized access and environmental hazards. The Open Text data centres where Processing, storage and communication equipment is installed are protected with the following security measures:

a) On-site security guards control and monitor access to the data centres 24 hours a day, 7 days per week.
b) Physical access control systems (including, but not limited to, named access lists, badge readers, physical keys and/or biometric controls) are installed at entry points to the data centre and areas within the data centre to restrict access. Personnel must pass an area where they are observed by security company personnel and access to the data centre through a circle lock/mantrap to prevent tailgating.
c) Within the data centre, sensitive areas are separated and are only accessible to personnel by use of their personal access control credentials, with the required privileges granted on a need-to-know basis and a legitimate business need approved by management.
d) Technical facility rooms are locked, and access control credentials are kept on site with issuance registration.
e) Emergency exterior door opening triggers an audible alarm when opened.
f) Third-party visitors and deliveries must be pre-announced, with access approved by listed approvers and visitors are escorted in the data centre.
g) A secure intermediate holding area is used for all deliveries. Delivery personnel does not have direct access to areas containing computer systems or communication facilities.
h) CCTV (video) surveillance and motion detection equipment is installed at key points in the facilities, including but not limited to, parking lots, reception areas and data centre rooms. Recordings are retained in line with applicable data privacy regulations.
i) Access is monitored by guard station personnel. Access reports and access privileges are reviewed by management.

System Access Control

This control describes the measures to prevent unauthorized logical access to Open Text data processing systems.

Production systems and networks have logical access controls in place and are segregated from corporate and public networks. Employee access rights are granted following the least privilege access principle, on a need-to-know basis and with legitimate business need. All access requests are validated by the information security personnel and approved by management. System authentication credentials assigned to individual Open Text personnel are solely for their own use. Authentication credentials must not be shared or disclosed to any third party. It is a breach of policy for any user to misuse their or other users' authentication credentials.
Passwords must comply to the password policy published in the Information Security Policy in terms of complexity which, as of the effective date of this document, are:

a) A 10-character minimum password must be utilized where supported.
b) Where system constraints exist, the maximum character length supported by the system configuration capabilities must be utilized.
c) Passwords must contain at least one alpha character in upper case, one in lower case, one numeric and one non-alphanumeric character.

And the following thresholds apply to Open Text corporate accounts:

a) Personal accounts will lock after six consecutive failed login attempts.
b) Personal accounts that are not utilized within 90 days will automatically become disabled.
c) Passwords for user accounts must be changed after their initial creation.

For access to production environments by Open Text personnel, secure logical access gates are in place and require multi-factor authentication. Recording of activities on production systems is done through logging and using software deployed on the access gates.

Regular validation of access privileges is performed by information security personnel and functional managers to control moves, adds or changes to privileges and accounts.
The Open Text Information Security Group maintains a centrally managed and monitored Universal Threat Management (UTM) solution in place, which has IDS/IPS capabilities.
Select facilities support data at rest encryption using Advanced Encryption System (AES) or greater.

Data Access Control

This control describes the measures to prevent data being read, copied, modified or deleted without authorization.

In addition to the Physical and System Access Controls described above, access to customer data is restricted according to principles of least privilege and stored within a secured environment.
All Production systems are operated in secure data centres or facilities. Security measures that protect systems Processing Personal Data are regularly checked. To this end, Open Text conducts internal and external security checks and penetration testing on its data processing infrastructure.
Installation of software on the Open Text network is subject to approval by the Open Text Global Information Security group.

Disclosure Control

This measure ensures that Personal Data is not accessible (for reading, copying, modification or deletion) when being electronically sent over public networks to other parties or stored on other data media, except as necessary for the provision of Services in accordance with the relevant Agreement.

A multi-layer security approach depends on maintaining appropriate security measures and procedures at five different levels within the production environment:

Perimeter

a) Perimeter firewall
b) Distributed Denial of Services (DOS) protections (in select facilities)
c) Private IP connection with customers is available for order by customers on a case-by-case basis

Network

a) Intrusion Detection System (IDS)/Intrusions Prevention System (IPS)
b) Vulnerability management system, both vulnerability scans and third-party penetration testing
c) Access control/User authentication, multi-factor authentication for access to the production environment
d) Load Balancer/VLAN filter deployment to control network access

Host

a) Hosts and virtual servers are hardened, including thread and Vulnerability Assessments
b) Load Balancer/VLAN filter deployment to control network access
c) Anti-virus/Anti-malware protections
d) Access control and user authentication

Application

a) Access control and user authentication

Data

a) Encryption of data in transit and data at rest (as set out in the Customer contract)
b) Access control/user authentication
c) Shielded (secured) replication to remote site for Disaster Recovery synchronization

Open Text networks and service environments are isolated from foreign networks. Network routers and switches are configured with strict access control lists to prevent uncontrolled routing and broadcasting of network routes. Firewalls are configured with ingress and egress filters and only allow access to select services on the multi layered production systems and networks.
To protect data in transit and provide secure communication in transit, inherent encryption is applied based on transmission protocol. End-user sessions from their browser to portal applications are encrypted with HTTPS by policy.
Disposal of redundant processing and storage equipment or media is accomplished following strict disposal procedures that include the use of certified data destruction processes and/or companies. Open Text removes all copies and instances of Customer data from Open Text's disk storage, backups and archives per NIST 800-88 or Department of Defense 5220.22-M standard protocols. Upon request, Open Text will certify in writing that all Customer data has been removed.

Input Control

Input control enables verification of when, where and by whom Personal Data in the Open Text systems has been entered, edited or deleted.

All access to information and systems by Open Text personnel is enforced through a least privileged access policy, a full, role-based, lifecycle for identity access management process and a regular cadence review and validation of all access privileges. Workforce members are only granted rights to access assets needed to fulfill job functions.

Change Control

In addition, all system changes must be recorded, verified, tested and approved following a change management process that is based on the Information Technology Infrastructure Library (ITIL) standard.

Availability Control

Through this control, the accidental destruction or loss of Personal Data is protected.

The Open Text data centre facilities are designed to physically protect equipment and other critical resources from unauthorized access and environmental hazards. Data centres are designed to meet industry standards and practices. All critical technical facilities such as power, cooling and networking are redundant with A+B feeds. The systems are proactively monitored 24 hours a day, 7 days a week.

Open Text performs regular risk assessments and recovery tests on at least an annual basis covering its business processes, systems or applications as appropriate.

Data Separation

Data collected for different purposes can be processed separately.

To ensure that data collected for different purposes can be processed separately, Open Text segregates its corporate and commercial operating environments.

Access from the corporate to commercial networks is provided through security gates that require multi-factor authentication, perform logging and whose access is provisioned via the centrally authorized Global Information Security Unit.

Data storage is logically segregated customer-by-customer with partitioning. All data segregation by tenant is engineered to ensure data is not commingled.

APPENDIX 4
EEA CONTROLLER TO PROCESSOR CLAUSES (MODULE 2)

This attachment is attached to and forms part of the Data Processing Addendum between Open Text and Customer ("DPA"). Unless otherwise defined in this attachment, capitalised terms used in this attachment have the meanings given to them in the DPA.

Swiss Amendments to the EEA Standard Contractual Clauses

In the case of a Swiss Restricted Transfer where these Controller to Processor standard contractual clauses apply, they shall be deemed 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) In Annex I.C 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, 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) Clause 18 (c) shall be interpreted to permit data subjects in Switzerland to bring legal proceedings in Switzerland.

Standard Contractual Clauses
(Transfer controller-to-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 Annex 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 Annex 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 Annex I.B.
d) The Appendix to these Clauses containing the Annexes referred to therein forms 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

1 Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

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:
   iii. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
   iv. Clause 8 – Clause 8.1(b), 8.9(a), (c), (d) and (e);
   v. Clause 9 – Clause 9(a), (c), (d) and (e);
   vi. Clause 12 – Clause 12(a), (d) and (f);
   vii. Clause 13;
   viii. Clause 15.1(c), (d) and (e);
   ix. Clause 16(e);
   x. Clause 18 – 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 Annex 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 Annex I.A.

b) Once it has completed the Appendix and signed Annex 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 Annex 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 Annex 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 Annex 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 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 Annex 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 Annex 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 Annex 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) 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 14 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.

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

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 Annex 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 Annex 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) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex 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 Annex 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.

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

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 noncompliance. 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 one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Netherlands.

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 the Netherlands.

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.

ANNEX I

A - LIST OF PARTIES

Where there is a Restricted Transfer, Customer is the Controller and Open Text is the Processor, then Customer is the data exporter and Open Text is the data importer.

See Principal Agreement for the following information in respect of each party: name; address; contact person's name, position and contact details.

See Description of Transfer Appendix of the DPA for activities relevant to the data transferred under these Clauses.

B - DESCRIPTION OF TRANSFER

See Description of Transfer Appendix of the DPA.

C - COMPETENT SUPERVISORY AUTHORITY

The supervisory authority shall be the competent supervisory authority that has supervision over the Customer in accordance with Clause 13 of the EEA Controller to Processor SCCs

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

See Technical and Organisational Measures of the DPA.

APPENDIX 5

EEA PROCESSOR TO PROCESSOR CLAUSES (MODULE 3)

This attachment is attached to and forms part of the Data Processing Addendum between Open Text and Customer ("DPA"). Unless otherwise defined in this attachment, capitalised terms used in this attachment have the meanings given to them in the DPA.

Swiss Amendments to the EEA Standard Contractual Clauses

In the case of a Swiss Restricted Transfer where these Processor to Processor standard contractual clauses apply, they shall be deemed 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) In Annex I.C 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, 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) Clause 18 (c) shall be interpreted to permit data subjects in Switzerland to bring legal proceedings in Switzerland.

Standard Contractual Clauses (Transfer Processor-to-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)[5] 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 Annex 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 Annex I.A (hereinafter each 'data importer')

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

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

d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

[5] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

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 – Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);
    iii. Clause 9 – Clause 9(a), (c), (d) and (e);
    iv. Clause 12 – Clause 12(a), (d) and (f);
    v. Clause 13;
    vi. Clause 15.1(c), (d) and (e);
    vii. Clause 16(e);
    viii. Clause 18 – 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 Annex 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 Annex I.A.

b) Once it has completed the Appendix and signed Annex 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 Annex 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 exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.
b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.
c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.
d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter[6].

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 Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or 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 personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand 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.

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 rectify or erase 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 Annex 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 controller 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

[6] See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

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, they 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 subject. 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 or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex 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 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, without undue delay, the data exporter and, where appropriate and feasible, the controller 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 data breach, including 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 its controller so that the latter may in turn 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 set out in Annex I.B.

8.8. Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union([7]) (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;

[7] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

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 or the controller 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 controller.
c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.
d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.
e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.
f) 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.
g) 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) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 14 days in advance, thereby giving the controller 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 controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).
b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), 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.([8]) 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 or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. 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.

[8] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

Clause 10

Data subject rights

a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.
b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex 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 controller, as communicated by 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 Annex I.C, shall act as competent supervisory authority.
b) 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) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.
c) 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 Annex I.C, shall act as competent supervisory authority.
d) 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;[9]
    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.

[9] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

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). The data exporter shall forward the notification to the controller.
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, if appropriate in consultation with the controller. 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 controller or 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.

   The data exporter shall forward the notification to the controller.
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.). The data exporter shall forward the information to the controller.
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. The data exporter shall make the assessment available to the controller.

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 and the controller of such noncompliance. 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 one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Netherlands.

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 the Netherlands.

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.

ANNEX I

A - LIST OF PARTIES

Where there is a Restricted Transfer, Customer is a Processor and Open Text is a Processor, then Customer is the data exporter and Open Text is the data importer.

See Principal Agreement for the following information in respect of each party: name; address; contact person's name, position and contact details.

See Description of Transfer Appendix of the Data Processing Addendum between Open Text and Customer ("DPA") for activities relevant to the data transferred under these Clauses.

B- DESCRIPTION OF TRANSFER

See Description of Transfer Appendix of the DPA.

C- COMPETENT SUPERVISORY AUTHORITY

The supervisory authority shall be the competent supervisory authority that has supervision over the Customer in accordance with Clause 13 of the EEA Processor to Processor SCCs.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

See Technical and Organisational Measures of the DPA.

APPENDIX 6

UK INTERNATIONAL DATA TRANSFER ADDENDUM

This attachment is attached to and forms part of the Data Processing Addendum between Open Text and Customer ("DPA"). Unless otherwise defined in this attachment, capitalised terms used in this attachment have the meanings given to them in the DPA.

Part 1: Tables

Table 1: Parties

Start date	Date of the DPA.	
The Parties	**Exporter (who sends the UK Restricted Transfer)**	**Importer (who receives the UK Restricted Transfer)**
Parties' details	Where there is a UK Restricted Transfer, Customer is either a Controller or Processor and Open Text is a Processor, then Customer is the data exporter (and Open Text is the data importer). See Principal Agreement for the following information in respect of each party: name; address; contact person's name, position and contact details.	Where there is a UK Restricted Transfer, Customer is either a Controller or Processor and Open Text is a Processor, then Open Text is the data importer (and Customer is the data exporter). See Principal Agreement for the following information in respect of each party: name; address; contact person's name, position and contact details.
Key Contact	See above.	See above.
Signature (if required for the purposes of Section 2)	N/A	N/A

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☐ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: N/A Reference (if any): N/A Other identifier (if any): N/A Or ☒ 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:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1 [controller to controller]	✕	✕	✕			
2 [controller to processor]	✓	✓	✕	General	14 days	
3 [processor to processor]	✓	✓	✕	General	14 days	
4 [processor to controller]	✕	✕	✕			✕

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the identity of the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: Identity and contact details of the Parties and, where applicable, of its/their data protection officer and/or representative in the European Union/United Kingdom are set out in the Principal Agreement and DPA.
Annex 1B: Description of Transfer: See Description of Transfer Appendix of the DPA.
Annex II: Technical and organisational measures, including technical and organisational measures to ensure the security of the data: See Technical and Organizational Measures of the DPA.
Annex III: List of Sub-processors (Modules 2 and 3 only): See Section 2.3.1 of the DPA.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☐ Importer ☐ Exporter ☒ Neither Party

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: 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.