OpenText Cloud
General Terms and Conditions ("GTC")
Multitenant Services

These OpenText Cloud General Terms and Conditions ("**GTC**") apply to the Services and will be binding on Customer and OT when OT makes any Services available for Customer's use. The term "**OT**" means Open Text Corporation or the Open Text entity providing the Service. By using the Services, you agree to these GTC. If you use or access the Services on behalf of a company or other legal entity, you represent that you have the authority to bind that company or other legal entity to these GTC. If you do not agree to these GTC, you should not use the Service.

1. DEFINITIONS.

1.1 "**Affiliate**" means any entity, directly or indirectly controlled by, controlling, or under common control with a party to the Agreement. If an entity ceases to meet these criteria, it shall cease to be an Affiliate under these GTC.

1.2 "**Agreement**" means the Order, these GTC and any other documents incorporated pursuant to the Order.

1.3 "**Applicable Taxes**" means the sales, use, consumption, goods and services, and value-added taxes applicable to the Services or Client Side Software, except taxes imposed on OT's income.

1.4 "**AUP**" means OT's Cloud Services Acceptable Use Policy available at https://www.opentext.com/agreements or upon request from OT.

1.5 "**Authorized User**" means any employee or contractor of Customer or other individual or entity who are authorized by Customer to access and use the Services or who use the Services under Customer's account. Authorized Users will be identified by Customer to OT.

1.6 "**Client Side Software**" means a specific piece of software that OT may permit Customer to download for use in conjunction with the Services.

1.7 "**Cloud Services**" means the products and services provided by OT under the Agreement and delivered online using cloud computing technology, as described in the Order or Documentation. Cloud Services may also include the use of Client Side Software on a subscription basis.

1.8 "**Confidential Information**" means any information disclosed by one party (the "**Disclosing Party**") to the other party (the "**Receiving Party**") which: (i) is marked as proprietary by the Disclosing Party; or (ii) the Receiving Party should reasonably understand to be confidential. Confidential Information does not include information that: (a) is independently developed by the Receiving Party, without reference to the Disclosing Party's Confidential Information; (b) is already in the Receiving Party's possession prior to receipt from the Disclosing Party; (c) is Content; or (d) is or becomes publicly available other than through violation of the Agreement.

1.9 "**Content**" means Customer's data uploaded, generated, stored, or transmitted by Customer to OT, as a part of Customer's use of the Services.

1.10 "**Covered Country**" means each contracting party to The Patent Cooperation Treaty (currently published at http://www.wipo.int/pct/en/).

1.11 "**Customer**" means the OT customer that is referenced on the Order.

1.12 "**Documentation**" means all written, electronic, online, and other documentation provided or made available by OT to Customer under the Agreement relating to the Cloud Services.

1.13 "**Evaluation Services**" means the Services offered by OT under these GTC and which are provided on a limited-use basis before Customer decides to purchase.

1.14 "**Infringement Claim**" means claims, suits, actions, or proceedings brought against Customer in a court of competent jurisdiction in a Covered Country by a third party which allege an infringement by the Services or Client Side Software of a third party's patent, copyright, or trade secret.

1.15 "**No Fee Services**" means the Services offered by OT under these GTC for which OT does not charge Customer a fee.

1.16 "**Order**" means the order for Services accepted by both parties which references these GTC.

1.17 "**Services**" means the Cloud Services which OT provides to Customer pursuant to the Agreement.

1.18 "**Support**" means the operational and technical support services applicable to the Services, as defined in the Order.

2. TERM. The Agreement will be effective on the date the Agreement is accepted by the parties and continue until the end of the period referenced in the Order. Renewals of the Agreement term shall be as set forth in the Order.

3. SERVICES.

3.1 OT will provide the Services to Customer pursuant to these GTC, the Order, and other documents referenced in the Order.

3.2 As reasonably necessary to reflect changes in its business, technology and service offerings, OT may change its rules of operation, access procedures, software, the Services or the Documentation. OT will provide notice of changes by posting

information concerning the changes via email or by notification directly through the Services (*e.g.*, on a Services login page or customer portal). If a change has a material adverse effect on Customer's use of the affected Services, OT will: (i) give reasonable advance written notice identifying the reason for the change and the expected impact prior to implementing such change; and (ii) consult with Customer to identify ways to mitigate the impact of any such change.

3.3 With regard to Client Side Software, if provided, Customer may use Client Side Software for the sole purpose of facilitating Customer's use of the Services.

3.4 Customer acknowledges that: (i) Client Side Software may include additional terms, as notified to Customer or its Authorized Users at the time of installation or use of the Client Side Software; and (ii) access to and use of any OT third party vendor's software as part of the Services may be subject to Customer agreeing to third party terms applicable to such software.

3.5 Some of the Services or Client Side Software may be designed to upload, download and synchronize files between Customer's computer or other devices and OT servers. By using the Services, Customer grants OT permission to access Customer's computer or other devices for the purpose of providing the Services.

3.6 When Customer's right to receive and use the Services terminates, Customer's rights to access and use (i) Client Side Software, and (ii) any OT third party vendor's software provided under the Services, shall also terminate. Upon such termination, Customer must (a) immediately destroy all copies of the Client Side Software and any OT third party vendor's software, and (b) immediately and, upon OT request, provide OT with written certification of such destruction.

4. CUSTOMER RESPONSIBILITIES.

4.1 Customer is responsible for: (i) obtaining, installing, and maintaining the equipment, communication lines and support services necessary to access the Services; and (ii) ensuring that its Internet or telecommunications connections (if applicable), hardware, devices and software are secure and compatible with the Services. If Customer elects to use a third party contractor to perform work interfacing with the Services, such work shall be subject to OT's prior written consent. Customer is solely responsible for any work performed by, and any acts or omissions of, such third party contractor.

4.2 Use of the Services may require Customer to create an administrator account for a Customer administrator. The Services may enable the Customer administrator to provision and register Customer's Authorized Users to access and use the Services. In addition, Authorized Users may need to individually register with OT to use the Services. Customer is responsible for keeping Authorized User registration information accurate, complete and up to date.

4.3 Customer shall be responsible for: (i) acts or omissions by its Authorized Users; (ii) maintaining the confidentiality of access credentials (including usernames, passwords, and keys) used by Customer or its Authorized Users; (iii) ensuring compliance with the Agreement by each Authorized User, including compliance with OT's AUP; and (iv) ensuring compliance with applicable local, state and national laws and regulations in connection with the use of the Services, including those related to export compliance, data privacy, international communications and the transmission of data. OT may suspend the Services without liability to OT in order to comply with applicable law, or to prevent damage to OT or its other customers. Upon written notice to Customer, OT may require Customer's assistance in verifying usage of the Services in compliance with the terms of the Agreement.

5. RESTRICTIONS ON USE.

5.1 Customer will only use the Services for Customer's internal business purposes. Only Customer's Authorized Users may access and use the Services.

5.2 Customer shall not: (i) resell the Services to third parties without OT's prior express written agreement; (ii) create multiple free accounts under different or fake identities or otherwise that enables Customer to exceed the usage limits associated with the Service; (iii) disclose to any third party the results of any benchmarking testing or comparative or competitive analyses of the Services done by or on behalf of Customer; or (iv) modify, reverse engineer, decompile or otherwise attempt to discover the source code of Client Side Software or any of OT's or its third party vendor's software that are included in the Services.

5.3 Customer: (i) does not have any rights to Client Side Software or to any of OT's or its third party vendors' software that are included in the Services, other than the use and access thereof as part of receiving the Services; and (ii) does not receive any title, license, rights or ownership in or to any of the foregoing.

6. INTELLECTUAL PROPERTY; CONTENT.

6.1 OT alone owns all right, title and interest, including all related intellectual property rights, in and to (i) the Services, (ii) the Documentation, (iii) Client Side Software, and (iv) any suggestions, ideas, requests, feedback, recommendations or other information provided by Customer or any other party relating to the foregoing, and OT reserves all rights to use, modify and allow others to use such materials. OT grants Customer a nonexclusive and non-transferable right to use such materials in connection with the Services. Customer may not remove OT's copyright or other proprietary notices from the Documentation or any part of the Services.

6.2 As between Customer and OT, Content belongs to Customer, and OT makes no claim to any right of ownership in the Content. Customer represents and warrants to OT that Customer is the owner of all rights to the Content, or that Customer has the right to reproduce, distribute and transfer the Content for the purposes of the Agreement.

6.3 OT will store and safeguard Content in accordance with the administrative, technical, and physical security controls and procedures as defined in the Agreement. Customer may not create or transmit Content that imposes a greater obligation on OT than as expressly set forth in the Agreement.

6.4 Customer remains solely responsible for the Content and for ensuring that the Content complies with the Agreement and with all legal and regulatory obligations applicable to the Content. Only to the extent necessary for OT to perform its obligations under the Agreement, Customer grants OT the right to use, copy, process, rename, publish or display Content, and OT may monitor, modify, screen, pre-screen or delete the Content, provided any such deletion or substantial modification of Content shall only be carried out by OT with Customer's consent or direction. Notwithstanding the foregoing, if any portion of the Content contains material that is harmful to OT's systems or the Content (for example a virus), OT reserves the right to act without Customer's consent to protect OT's systems and the Content.

6.5 With respect to Content, any applicable data retention period and/or any data return service provided with the Services, as well as any fees payable by Customer therefor, will be specified in the Agreement. OT shall have no obligation to retain or delete Content or to return Content to Customer except as provided in the Agreement. For Evaluation Services or No Fee Services, Content may be deleted by OT immediately without any retention period or notice.

6.6 Provided Customer is not in material breach of the Agreement and is current with payment obligations, and subject to the requirements of the Services, Customer may access or delete Content at any time prior to the expiration or termination of the Agreement term. When an Agreement term expires or terminates, Content that Customer has not previously deleted or removed will be retained for at least 30 days. Customer remains responsible for all storage and other applicable charges during this retention period. Unless otherwise stated in the Agreement, OT may delete all Content contained on primary (*i.e.,* non-backup) storage, after 30 days following the expiration or termination of the Agreement term. Following termination, OT may retain Content on backup media for an additional period of up to 12 months, or longer if required by law, subject to the confidentiality obligations under these GTC.

6.7 Customer will be responsible for the correctness and completeness of any programs, files, data, or other materials to be provided to OT for use in the provision of Services. Customer shall ensure that OT has the right to use such materials for the purpose of performing its obligations under the Agreement.

7. DATA PROTECTION.

7.1 OT will provide the Services in accordance with privacy and data protection laws, to the extent applicable to OT. OT's Privacy Policy is located at https://www.opentext.com/who-we-are/copyright-information/site-privacy.

7.2 To the extent that OT processes personal data on behalf of Customer in performing the Services: (i) OT shall implement reasonable and appropriate technical and organizational measures designed to protect personal data against unauthorized or unlawful processing; (ii) OT shall not collect, sell or use such personal data except as necessary to perform the Services, or as otherwise permitted by the applicable laws; and (iii) where an individual submits a verifiable request to OT to exercise their privacy rights relating to their personal data in respect of a named Customer, OT shall forward these requests to the named Customer's email address on file with OT as soon as reasonably practicable.

7.3 OT may employ its Affiliates and third parties worldwide in the performance of the Services, provided that OT shall remain primarily responsible to Customer.

7.4 To the extent that OT requires personal data to provide the Services, Customer will provide personal data only to the extent reasonably required. Customer is responsible for implementing and maintaining privacy protections and security measures for components that Customer provides or controls, as well as complying with its obligations under this Agreement or otherwise required by law.

8. TERMINATION OF THE AGREEMENT.

8.1 For cause; Evaluation and No Fee Services. A party may terminate the Agreement for material breach by the other party if the other party fails to cure such breach within 30 days after written notice. For material breaches relating to the rights granted or restrictions in Sections 4 (CUSTOMER RESPONSIBILITIES), 5 (RESTRICTIONS ON USE) or 13 (CONFIDENTIALITY), no such cure period will be granted and such termination may be immediate. Except in the event of a material breach or as specifically provided in these GTC or an Order, neither party will be permitted to terminate the Agreement prior to the end of the term set forth in the Order or any mutually agreed renewal term applicable thereto. Either party may terminate the Agreement and any Services at any time with respect to Evaluation Services or No Fee Services by giving at least thirty (30) days' written notice. OT reserves the right to terminate and delete any Customer Content related to Evaluation Services or No Fee Services if Customer has not accessed the Service for 12 or more consecutive months.

8.2 Actions upon termination. Upon any termination of the Agreement, Customer will immediately either deliver to OT or destroy all copies of (i) Documentation, (ii) Client Side Software, and (iii) any of OT's third party vendor's software that is included in the Services, which are in Customer's possession or control.

8.3 Survival. The following provisions of these GTC shall survive termination or expiration of the Agreement Sections: 5 (RESTRICTIONS ON USE); 6 (INTELLECTUAL PROPERTY; CONTENT); 9 (FEES, PAYMENT AND TAXES); 10 (WARRANTIES); 11 (INFRINGEMENT INDEMNITY); 12 (LIMITATION OF LIABILITY); 13 (CONFIDENTIALITY); and any provisions that by their nature should survive termination.

9. FEES, PAYMENT AND TAXES.

9.1 Customer shall pay OT the fees and charges specified in the Order including any applicable overage charges. Fees are exclusive of any Applicable Taxes or import duties due as a result of amounts paid to OT or the performance of the Services. OT may offer: (i) different categories of paid subscriptions to the Services; (ii) subscriptions for Evaluation Services; and (iii) subscriptions for No Fee Services.

9.2 OT will submit invoices against the Order for ongoing provision of the Services.

9.3 The fees and charges are subject to a five percent (5%) increase which will be applied annually during the initial committed term (as set forth in the Order), and during each subsequent renewal term on the anniversary of the date on which such fees and charges came into effect.

9.4 Payments are due 30 days from the date of invoice. Invoices shall be issued as set forth in the Order. Fees and other charges owed by Customer not paid when due shall accrue interest at the lesser of one and one-half percent (1.5%) per month or the highest rate permitted by law. Customer shall bear all of OT's costs of collection of overdue fees, including reasonable attorneys' fees.

9.5 If an invoice remains unpaid following at least 10 days written notice by OT, OT may (reserving all other legal remedies and rights) suspend the Services or, following 30 days written notice by OT, terminate the Agreement.

9.6 If OT is unable to charge Customer's payment method (*e.g.,* due to the expiration of a credit card), Customer is still obliged to pay OT the amounts to which Customer has committed under the Agreement. All fees are non-refundable. Customer is solely responsible for any fees imposed by its credit card company, including exchange rate or foreign transaction fees.

10. WARRANTIES.

10.1 OT warrants that the Services will be rendered in a professional and workmanlike manner and will function, in all material respects, in conformance with the Order.

10.2 EXCEPT AS EXPRESSLY PROVIDED IN THE AGREEMENT, THE SERVICES, SOFTWARE, DELIVERABLES AND DOCUMENTATION ARE PROVIDED WITHOUT EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, OT DISCLAIMS ALL OTHER WARRANTIES AND CONDITIONS, INCLUDING ANY IMPLIED WARRANTIES OR CONDITIONS OF SATISFACTORY QUALITY, OF MERCHANTABILITY OR OF FITNESS FOR A PARTICULAR PURPOSE OR THOSE ARISING BY LAW, STATUTE, USAGE OF TRADE OR COURSE OF DEALING. OT DOES NOT WARRANT THAT THE SERVICES WILL BE ERROR FREE OR WILL OPERATE WITHOUT INTERRUPTION. CUSTOMER ASSUMES THE RESPONSIBILITY TO TAKE ADEQUATE PRECAUTIONS AGAINST DAMAGES TO ITS CONTENT OR OPERATIONS WHICH COULD BE CAUSED BY SERVICES DEFECTS, INTERRUPTIONS, OR MALFUNCTIONS.

10.3 If Customer chooses to use any Evaluation Services or No Fee Services, Customer may do so only: (i) subject to the limitations defined for such Services; and (ii) if applicable, to evaluate functionality, performance, compatibility and reliability during the specified period. In connection with such use, Customer specifically agrees that: (a) Evaluation Services and No Fee Services are provided "AS-IS" and without support; and (b) any security, compliance, service level, and privacy commitments made by OT in connection with the Agreement are not applicable to Evaluation Services or No Fee Services.

11. INFRINGEMENT INDEMNITY.

11.1 Provided Customer is not in material breach of the Agreement and is current with payment obligations, OT will defend Customer from any Infringement Claim, to the extent it arises solely from Customer's use of the Services in accordance with the provisions of the Agreement. This defense will not apply to an Infringement Claim to the extent caused by: (i) modification of the Services by any party other than OT; or (ii) the combination or use of the Services with software, hardware, firmware, data, or technology not provided by OT to Customer. As to any such Infringement Claim referenced under the preceding items (i) or (ii), OT assumes no liability for infringement and Customer will hold OT harmless against any infringement claims arising therefrom. OT will not defend, indemnify or hold harmless a Customer from any Claims or other liabilities, damages or losses arising in connection with any Evaluation Services or No Fee Services.

11.2 OT's obligations in this Section are conditioned upon: (i) Customer notifying OT in writing within 10 days of Customer becoming aware of an Infringement Claim; (ii) Customer not making an admission against OT's interests; (iii) Customer not agreeing to any settlement of an Infringement Claim without the prior written consent of OT; (iv) Customer providing reasonable assistance to OT in connection with the defense, litigation, and settlement by OT of the Infringement Claim; and (v) OT's sole control over legal counsel, litigation and settlement of each Infringement Claim. OT will indemnify Customer from any judgment finally awarded, or in settlement of, any Infringement Claim where all the conditions of this Section are satisfied.

11.3 If the Services become, or in OT's opinion may become, the subject of an Infringement Claim, OT will, at no expense to Customer: (i) obtain a right for Customer to continue using the Services; (ii) modify the Services so they become non-infringing but still provide substantially the same functionality as the infringing Services; or (iii) terminate the Services and refund the unused portion of any prepaid fees received by OT from Customer. OT's entire liability and Customer's sole and exclusive remedy with respect to any Infringement Claim shall be limited to the remedies set forth in this Section 11.

11.4 Customer shall defend, indemnify and hold harmless OT, its affiliates, directors and employees from any damages, losses, claims and expenses arising from any claim or other legal action related to: (i) Content which OT uses, processes and/or manages in connection with the Services; (ii) Customer's or any Authorized User's use of the Services; (iii) Customer's or any Authorized User's breach of these GTC; and (iv) Customer's or any Authorized User's breach of the AUP.

12. LIMITATION OF LIABILITY.

12.1 EXCLUSION OF DAMAGES. OT AND ITS AFFILIATES ARE NOT LIABLE TO CUSTOMER OR TO ANY OTHER PARTY FOR: (A) ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, AGGRAVATED, EXEMPLARY, OR

PUNITIVE DAMAGES; OR (B) ANY LOST SALES, LOST REVENUE, LOST PROFITS, LOST OR CORRUPTED DATA, OR REPROCUREMENT AMOUNT; OR (C) FORCE MAJEURE UNDER SECTION 14.10 BELOW.

12.2 LIMITATION OF LIABILITY. THE LIABILITY OF OT AND ITS AFFILIATES WILL NOT EXCEED, IN THE AGGREGATE: (A) 50% OF THE TOTAL AMOUNT OF FEES INVOICED BY OT TO CUSTOMER UNDER THE AGREEMENT DURING THE 12 MONTH PERIOD PRECEDING THE OCCURRENCE OF THE APPLICABLE CLAIM; AND (B) A MAXIMUM AMOUNT FOR ALL CLAIMS DURING THE TERM OF THE AGREEMENT OF THE TOTAL AMOUNT OF FEES INVOICED BY OT TO CUSTOMER DURING THE 12 MONTH PERIOD PRECEDING THE MOST RECENT EVENT WHICH IS THE CAUSE OF LIABILITY UNDER THE AGREEMENT. WITH RESPECT TO EVALUATION SERVICES AND NO FEE SERVICES AND RELATED SOFTWARE, NEITHER OT NOR OT'S SUPPLIERS, RESELLERS, PARTNERS OR THEIR RESPECTIVE AFFILIATES WILL BE LIABLE FOR DIRECT DAMAGES.

12.3 DISCLAIMER. THE LIMITATIONS IN THIS SECTION APPLY IN REGARD TO ANY AND ALL CLAIMS ARISING OUT OF OR RELATING TO THE AGREEMENT OR THE SERVICES, IN TORT, EQUITY, AT LAW, STRICT PRODUCT LIABILITY, OR OTHERWISE, INCLUDING CLAIMS OF NEGLIGENCE, BREACH OF CONTRACT OR WARRANTY, REGARDLESS OF THE FORM OF ACTION, EVEN IF: (A) OT IS ADVISED IN ADVANCE OF THE POSSIBILITY OF THE DAMAGES IN QUESTION; (B) SUCH DAMAGES WERE FORESEEABLE; OR (C) CUSTOMER'S REMEDIES FAIL IN THEIR ESSENTIAL PURPOSE. IF THE APPLICATION OF THIS SECTION 12 IS LIMITED BY LAW, THE LIABILITY OF OT AND ITS AFFILIATES WILL BE LIMITED TO THE EXTENT PERMITTED BY LAW. NOTHING IN THIS AGREEMENT SHALL EXCLUDE OR LIMIT EITHER PARTY'S LIABILITY FOR: (I) DEATH OR PERSONAL INJURY CAUSED BY NEGLIGENCE; (II) FRAUD OR DECEIT; OR (III) ANY OTHER LIABILITY THAT CANNOT BE EXCLUDED BY APPLICABLE LAW. THE REMEDIES SPECIFIED IN THE AGREEMENT ARE EXCLUSIVE.

13. CONFIDENTIALITY. Each Disclosing Party may disclose to the Receiving Party Confidential Information pursuant to the Agreement. Each Receiving Party agrees, for the term of the Agreement and for three (3) years after such term, to hold Disclosing Party's Confidential Information in strict confidence, not to disclose such Confidential Information to third parties (other than to Affiliates and to professional advisers who are bound by appropriate written obligations of confidentiality) unless authorized to do so by Disclosing Party, and not to use such Confidential Information for any purpose except as expressly permitted hereunder. Each Receiving Party agrees to take reasonable steps to protect Disclosing Party's Confidential Information from being disclosed, distributed or used in violation of the provisions of this Section. The foregoing prohibition on disclosure of Confidential Information shall not apply to any information that: (i) is or becomes a part of the public domain through no act or omission of Receiving Party; (ii) was in Receiving Party's lawful possession without confidentiality obligation prior to the disclosure and had not been obtained by Receiving Party either directly or indirectly from Disclosing Party; (iii) is lawfully disclosed to Receiving Party by a third party without restriction on disclosure; (iv) is independently developed by Receiving Party or its employees or agents without use of Disclosing Party's Confidential Information; or (v) is required to be disclosed by Receiving Party as a matter of law or by order of a court or by a regulatory body, provided that Receiving Party promptly notifies Disclosing Party (where lawfully permitted to do so) so that Disclosing Party may intervene to contest such disclosure requirement and/or seek a protective order or waive compliance with this Section. Each Receiving Party is responsible for any actions of its Affiliates, employees and agents in breach of this Section.

14. MISCELLANEOUS.

14.1 Authority. If an individual uses or accesses the Services on behalf of a company or other legal entity, that individual represents that they have the authority to bind that company or other legal entity to these GTC. If such company or other legal entity does not agree with these GTC, the Services should not be used on its behalf.

14.2 Entire agreement and order of precedence. The Agreement represents the entire agreement of the parties, and supersedes any prior or current understandings, whether written or oral with respect to the subject matter of the Agreement. In the event of a conflict between the components of the Agreement, the Order will prevail over these GTC.

14.3 Amendment, waiver. Any amendment of the Agreement must be in writing and signed by both parties. Neither party will be deemed to have waived any of its rights under the Agreement by lapse of time or by any statement or representation other than by a written waiver by a duly authorized representative. No waiver constitutes a waiver of any prior or subsequent breach.

14.4 Governing law; time limit. The Agreement is governed by the laws of England and Wales without reference to its choice or conflicts of law rules. The parties consent to the exercise of exclusive jurisdiction by the courts in England and Wales for any claim relating to the Agreement. No action, regardless of form, arising from the Agreement or any Services provided or to be provided hereunder may be brought by either party more than two (2) years after the cause of action has accrued, except that an action for non-payment may be brought at any time.

14.5 Third Party Rights. The Agreement is also made for the benefit of OT's Affiliates. Except as expressly provided in this clause, or otherwise in the Agreement, the Agreement does not give rise to any rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of the Agreement.

14.6 Relationship of the parties. The relationship of the Parties created by the Agreement is that of independent contractor and not that of employer/employee, principal/agent, partnership, joint venture or representative of the other. Neither party is authorized to make any representation, contract or commitment on behalf of the other party. The establishment of the terms of any commercial or legal relationship between Customer and any third party by means of the use of the Services provided hereunder is the sole responsibility of Customer. The provision of such Services by OT will not be interpreted as conferring

any authority or responsibility on OT with respect to such relationships or the establishment, continuation or binding effect of such terms.

14.7 Services Statistics. Customer agrees that OT may gather and utilize statistical information gathered in connection with the Services and the data processed by the Services (the "Services Statistics"), however, OT will only utilize the Services Statistics: (i) in a manner that will not identify Customer as the source thereof; (ii) in a form where the data is anonymized; and (iii) in compliance with all applicable laws and regulations.

14.8 Assignment. There are no third-party beneficiaries to the Agreement. Customer may not assign or otherwise transfer any of its rights or obligations under the Agreement, in whole or in part, without the prior written consent of OT. Any assignment in breach of this Section is null and void. Except to the extent identified in this Section, the Agreement will be binding upon and inure to the benefit of the respective successors and assigns of the parties.

14.9 Export laws. The Services (which for purposes of this Section include any Client Side Software, Documentation and technical data stored or transmitted via the Services) may be subject to export control laws of the United States or other countries. Customer agrees to comply strictly with all applicable export regulations, including, but not limited to (i) the Export Administration Regulations maintained by the U.S. Department of Commerce, and (ii) the trade and economic sanctions maintained by the U.S. Department of Treasury Office of Foreign Assets Control, and will not allow use of the Services in a manner that breaches or facilitates the breach of such regulations. Customer has the responsibility to obtain any licenses required to export, re-export, or import the Services, including deemed exports. The Services shall not be used by anyone: (a) located in U.S. embargoed countries or by any Foreign National of a U.S. embargoed country; or (b) included on the U.S. Treasury Department's list of Specially Designated Nationals; or (c) the U.S. Department of Commerce's Denied Persons or Entity List. By using the Services, Customer represents and warrants that neither Customer nor any person provided access to the Service by Customer is located in any such country or on any such list.

14.10 Force Majeure. OT does not control the flow of data to or from the Services. Rather, such flow depends in large part on the performance of Internet services and technology provided or controlled by third parties and the public Internet infrastructure, as well as on other events beyond OT's control. At times, the action or inaction of parties or systems not controlled by OT or other events beyond OT's control can impair, disrupt or delay OT's ability to provide the Services or Customer's ability to access the Services. Notwithstanding anything to the contrary in the Agreement, OT disclaims, and Customer shall not hold OT responsible for, any and all liability resulting from or related to such actions or events, including acts of God, acts of governmental authority, unavailability of third party communication facilities or energy sources, fires, transportation delays, or any cause beyond the reasonable control of OT (collectively "**Force Majeure**").

14.11 U.S. Government End Users – Restricted Rights Legend. The Services and Documentation provided to the U.S. Government are "Commercial Items", as that term is defined at 48 C.F.R. 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", within the meaning of 48 C.F.R. 12.212 or 48 C.F.R.227.7202, as applicable. Consistent with 48 C.F.R. 12.212 or 48 C.F.R. 227.7202-1 through 227.7202-4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein, as provided in FAR 12.212, and DFARS 227.7202-1(a), 227.7202-3(a), 227.7202-4, as applicable.

14.12 Notices. All notices must be in writing and given by nationally recognized courier service, or electronic transmission and addressed to the law department at the address specified in the Order (as updated from time to time by either party giving notice to the other in writing) and will be effective upon receipt.

14.13 Publicity. OT may include Customer's name in a list of OT customers, whether online or in promotional materials.

14.14 Severability. If any provision of the Agreement is held by a court of competent jurisdiction to be contrary to law, the provision shall be modified by the court and interpreted so as best to accomplish the objectives of the original provision to the fullest extent permitted by law, and the remaining provisions of the Agreement shall remain in effect.

14.15 Governing language. The Agreement shall be prepared and interpreted in the English language. Any translation of the Agreement into another language is for the purpose of convenience only. Any inconsistency arising due to translation into another language or a difference of interpretation between two or more languages, will be resolved in favor of the English language version.

OpenText Core Applications & Services

Supplemental Terms

These additional terms of service ("**Supplemental Terms**") apply to the use of and access to the Core-branded Cloud Services ("**Core Cloud Services**") provided by "**OpenText**" meaning Open Text Corporation or the Open Text entity providing the Core Cloud Services. Use of the Core Cloud Services is subject to these terms, and either (a) the OpenText Cloud General Terms and Conditions Multitenant Services published on opentext.com/agreements ("**Online GTC**") or (b) a mutually agreed and executed contract between OpenText and Customer specifically noted on the ordering document, which shall supersede the Online GTC ("**Agreement**"). All references herein to GTC shall mean either the Online GTC or Agreement, whichever is applicable.

These Supplemental Terms may be updated from time to time by OpenText. Any capitalized terms not defined in these Supplemental Terms are defined in the GTC and are agreed to by the individual or legal entity who subscribes to Core Cloud Services ("**Customer**").

Tenants

Authorized Users of Core Cloud Services are provided access to one or more Core Cloud Services application tenants or service APIs as indicated in one or more schedules ancillary to this document ("Schedule(s)").

Data Center Regions

The primary data zone for customers of Core Cloud Services located in Europe, Africa and the Middle East ("**EMEA**") as indicated by the Customer address on the order is the EMEA data center region.

The primary data zone for customers located in North America, South America, and the Asia-Pacific region as indicated by the Customer address on the Order is the USA data center region.

Accounts

OpenText will enable an administrator account for the Customer-purchased Core Cloud Services using the contact information provided by the Customer, thus providing access to the application tenant(s) via this account to the Authorized User that Customer designates as the administrator of their account. Access credentials will be provided to the administrator by email. It is the Customer's responsibility to notify OpenText of changes to the contact details for the administrator.

Pursuant to the Schedule for the Core Cloud Services purchased, the administrator may provision a number of additional Authorized User accounts. An email address will be the user ID for each Authorized User provisioned. Only one Authorized User may be associated with any single, unique email address. Customer agrees to keep such account provisioning information accurate, complete, and up to date.

Support

Support for Core Cloud Services is described in the Cloud Support Program Handbook for Multitenant Services published on opentext.com/agreements ("**Cloud Handbook**").

Maintenance Activities

Customer acknowledges that OpenText will from time to time during the term of the Core Cloud Services be required to temporarily reduce or interrupt access to the Core Cloud Services for the purpose of maintaining or Updating the Services, as provided in the Cloud Handbook("**Routine Maintenance**"). OpenText publishes a Routine Maintenance Schedule (available via the Customer Service Portal(My Support) located at https://support.opentext.com) detailing the regular cadence of reserved maintenance windows, whichare available for use upon advance notice from OpenText to Customer.

OpenText and Customer also may mutually agree to conduct maintenance or implement changes on the Core Cloud Services outside of the predefined Routine Maintenance windows (conduct "**Scheduled Customer Maintenance**). OpenText may temporarily limit or suspend the availability of all or part of the Core Cloud Services if it is necessary to conduct emergency maintenance to action an urgent situation that could not have been prevented by OpenText using IT industry standard practices and preventive measures described in this Agreement for reasons of public safety, interoperability of services, data protection; or to perform work that is immediately necessary for operational, technical or security reasons ("**Emergency Maintenance**").

Service Level Agreement

OpenText shall endeavor to operate the Core Cloud Services in such a manner that they are available to Customer for a specific amount of time each month (expressed as a percent); seven days per week, 24 hours per day (the "**Target Service Availability**" or "**TSA**").

The TSA for Core Cloud Services is 99.9%.

The actual service availability ("**Actual Service Availability**" or "**ASA**") is measured as the ability to login to the internet available, production application tenant of each individual Core Cloud Service purchased and shall not apply Client Side Software (if any) operating on any device used by Customer to access the Core Cloud Services.

The calculation of ASA shall be based on the total minutes during a calendar month minus Downtime divided by the total minutes during a calendar month, where "**Downtime**" is the total time the service is unavailable adjusted in accordance with the downtime exclusions indicated below, or:

$$100\% - \frac{Downtime\ minutes}{minutes\ of\ service\ in\ the\ month} = Actual\ Service\ Availability\ \%$$

Upon Customer request OpenText will, subject to the terms herein, issue a credit payment based on the difference between the TSA and the ASA multiplied by the Monthly Fee (where the "**Monthly Fee**" is the portion of the fees paid for the particular Core Cloud Service that are applicable to the month the failed service availability was measured in). OpenText will issue Customer the credit payment annually in arrears if applicable.

For clarity, this calculation is illustrated in the examples below.

Target Service Availability	Actual Service Availability	Result	Percentage of Monthly Fee as Credit
99.9%	100%	0.1% exceeded	0%
99.9%	99.5%	0.4% missed	0.4%
99.9%	94.9%	5% missed	5%

The maximum amount of any credit for a calendar month for failure to meet the TSA may not exceed ten (10%) percent of Monthly Fees. OpenText's records and data shall be the basis for all remedy calculations. Customer must notify OpenText of their desire to claim credits within 90 days of the event giving rise to such credit.

The ASA will be based upon the results of tests executed by OpenText on a regular cadence every few minutes. The ASA will be adjusted to exclude impacts to Core Cloud Services availability caused by the following:

- Maintenance Activities
- Service interruptions or disruptions caused by Customer or Customer-controlled components
- Service interruptions not caused by OpenText or not within the control of OpenText (i.e. unavailability due to problems with the Internet), unless caused by OpenText's service providers
- Service interruptions caused by disruptions attributable to force majeure events (i.e. unforeseeable events outside of OT's reasonable control and unavoidable even by the exercise of reasonable care)
- Customer exceeding the service restrictions, limitations, or metrics of the measured Core Cloud Service
- Service downtime requested by Customer; or
- Suspensions of Service by OpenText as a result of Customer's breach of the agreed terms.

Customer's rights described in this section state Customer's sole and exclusive remedy for any failure by OpenText to meet the service levels.

Customer may terminate the Order if OpenText fails to meet the TSA such that the Customer is entitled to ten percent credit (a) during three (3) consecutive months or (b) during at least five (5) months (consecutive or not) over a twelve (12) month period. Such termination will be deemed termination for Cause. In the event that the Customer terminates the Order under this clause, OpenText will refund the portion of the prepaid fees (if any) attributable to Core Cloud Services not received by Customer.

Backup & Recovery

The Content associated with Core Cloud Services is backed up on a regular basis in accordance with OpenText's disaster recovery procedure.

In the event OpenText declares a disaster event that impacts delivery of the Core Cloud Services from the primary location, OpenText will restore service in an alternate location. The target recovery time objective ("**RTO**") following an OpenText declared disaster is 72 hours and the target recovery point objective ("**RPO**") is 4 hours.

Invoicing

OpenText will invoice Customer annually in advance for the Core Cloud Services described in the Order unless stated otherwise. OpenText will invoice Customer in arrears for applicable overage charges (if any).

Renewal

The initial Core Cloud Services subscription term begins on the Order date. After the initial subscription term, the Order will automatically renew annually, unless a party terminates the Order by notifying the other party in writing no less than thirty (30) days prior to the expiration of the then-current term.

Client Side Software

The following additional terms apply to the use of the Client Side Software provided by OT under the Order and described further in a Schedule:

1. **Ownership of Client Side Software.** OT alone owns all right, title and interest, including all related intellectual property rights, in and to Client Side Software and Customer does not receive any title, license, rights or ownership in or to any of the foregoing, except for the right to use the Client Side Software for the sole purpose of facilitating Customer's use of the Core Cloud Service.
2. **Software and Documentation**. Customer may make as many copies of the Client Side Software necessary for it to use the Client Side Software as permitted under the Order and/or the Schedule. Each copy of the Client Side Software made by Customer must contain the same copyright and other notices that appear on the original copy. Customer will not modify the Documentation related to the Client Side Software. Such Documentation may: (a) only be used to support Customer's use of the Client Side Software; (b) not be republished or redistributed to any unauthorized third party; and (c) not be distributed or used to conduct training for which Customer, or any other party, receives a fee. Customer will not copy any system schema reference document related to the Client Side Software.
3. **General Restrictions**. Except as provided in the Order and/or the Schedule, Customer will not and will not permit any other party to: (a) assign, transfer, give, distribute, reproduce, transmit, sell, lease, license, sublicense, publicly display or perform, redistribute or encumber the Client Side Software by any means to any party; (b) rent, loan or use the Client Side Software for service bureau or time-sharing purposes, or permit other individuals or entities to create Internet "links" to the Client Side Software or "frame" or "mirror" the Client Side Software on any other server or wireless or Internet-based device, or in any other way allow third parties to access, use, and/or exploit the Client Side Software; (c) use the Client Side Software, in whole or in part, to create a competitive offering; (d) charge a fee to any party for access to or use of the Client Side Software; (e) use the Client Side Software in a manner inconsistent with the Order and/or the Schedule.
4. **Derivative Works / Improvements**. Customer is prohibited from using the Client Side Software to create any change, translation, adaptation, arrangement, addition, modification, extension, upgrade, update, improvement, (including patentable improvements), new version, or other derivative work of or to the Client Side Software. Notwithstanding the foregoing, if any of the Client Side Software is provided to Customer in source code format (or any other format that can be modified), the Customer may modify such portion of the Client Side Software for the sole purpose of using the Client Side Software in accordance with the Order and/or the Schedule, and OT will solely own all modified portions and Customer will irrevocably assign to OT in perpetuity all worldwide intellectual property and any other proprietary rights in and to any modifications of the Client Side Software.
5. **Interfacing with Client Side Software**. Customer may not permit any software products not provided by OT to interface or interact with the Client Side Software, unless accomplished through the use of application program interfaces provided by OT.
6. **Verification**.
    i. During the term of the Order and for 24 months after, Customer will maintain electronic and other records sufficient for OT to confirm that Customer's use of the Client Side Software has complied with the Order and/or the Schedule. Customer will promptly and accurately complete and return (within 30 days of OT request) any self-audit questionnaires, along with a certification by an authorized representative of Customer

confirming that Customer's responses to the questionnaire accurately and fully reflect Customer's usage of the Client Side Software. OT may once per year audit Customer's records and computer systems (including servers, databases, and all other applicable software and hardware) to ensure Customer has complied with the Order. Customer shall cooperate with OT and promptly and accurately respond to, database queries, location information, system reports, and other reports requested by OT and provide a certification by an authorized representative of Customer confirming that information provided by Customer accurately reflects Customer's usage of the Client Side Software.

ii. Audits will be conducted during regular business hours and will not interfere unreasonably with Customer's business. OT will provide Customer prior notice of each audit. Such audit shall be scheduled as soon as reasonably possible but in no event more than 7 days subsequent to the notice. Customer will allow OT to make copies of relevant Customer records. OT will comply with all applicable data protection regulations.

iii. If Customer is not in compliance with the Client Side Software rights granted in the Order, Customer will be deemed to have acquired additional OT software licenses at OT's then-current license price to bring Customer into compliance, and Customer must immediately pay the applicable license fees, and support and maintenance fees for: (i) the period Customer was not in compliance with the Client Side Software subscription; and (ii) the first year support and maintenance sees on any additional Client Side Software, plus reasonable costs incurred by OT in performing the audit. Compliance with the Client Side Software terms and conditions is the sole responsibility of Customer.

Use of Third-Party Cloud Infrastructure

OpenText may use a third-party cloud infrastructure provider to provide portions of the Core Cloud Services. Obligations related to security are held as shared obligations by OpenText and such third-party cloud infrastructure vendor, as applicable (for example, OpenText may provide copies of the third-party cloud infrastructure vendors security reports or certifications to Customer regarding the portion of the Core Cloud Services they provide). Access to such reports or other audit activities requested by Customer, or any data protection authorities having jurisdiction over Customer, may be limited in scope to that allowed by such third-party cloud infrastructure provider and may be subject to additional charges which will be the responsibility of Customer. If Customer intends to utilize a third-party auditor, OpenText or its third-party cloud infrastructure provider may object in writing to such auditor where such auditor is not (i) reasonably qualified; or (ii) independent; or (iii) a competitor of OpenText or such third-party cloud infrastructure provider. Where Customer requires specific functionality which requires any additional processing service offered by a third-party cloud infrastructure provider (such as online language translations services), such additional services may be subject to the additional terms and restrictions of such third-party cloud infrastructure provider which shall be deemed to be incorporated herein. OpenText shall make available such additional terms to Customer prior to the implementation of such functionality. A third-party cloud infrastructure provider shall be considered asub-processor. Such third-party infrastructure provider may utilize sub-contractors provided that such use shall be subject tothe limitations set forth in this agreement.

The Core Cloud Services are not intended to be used for (i) activities where the failure of the Core Cloud Services could lead to death, serious personal injury, or severe environmental or property damage, and (ii) materials or activities that are subject to the International Traffic in Arms Regulations (ITAR) maintained by the United States Department of State. Any use of the Core Cloud Services for such activities by Customer will be at Customer's own risk, and Customer will be solely liable for the results of any failure of the Core Cloud Services when used for such activities.

If Customer processes personal information of any individuals, including without limitation, information concerning the health of any individuals, Customer represents and warrants that it has obtained any required consent of such individuals under applicable law. Customer will take appropriate measures to limit its use of such information within the Core Cloud Services tothe minimum extent necessary for Customer to carry out its authorized use of such information.

Open Text Data Processing Addendum

Parties

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

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

(2) the other party to the Principal Agreement ("**Customer**").

Open Text and Customer hereinafter separately referred to as “Party” and jointly as “Parties”.

Part A: Background and Introductory Matters

1 **Background**

1.1 This DPA (including its Appendices) supplements and forms part of the agreement between Open Text and Customer under which Open Text 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.

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

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.

1.4 If there is any conflict between the provisions of this DPA and the provisions of the Standard Contractual Clauses, the Parties agree that 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 clauses 5 and 13, such specifications also apply in relation to, and satisfy Customer rights under the respective provisions of the Standard Contractual Clauses.

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.

2 **Definitions**

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

2.1.1 "**Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with a 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;

2.1.2 "**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)

the data protection or privacy laws of Switzerland, in each case, to the extent applicable to the Processing of Personal Data under this DPA and the Principal Agreement;

2.1.3 "**EEA Standard Contractual Clauses**" means the EEA Controller to Processor SCCs and EEA Processor to Processor SCCs (each as amended, updated or replaced by European Commission from time to time);

2.1.4 "**EEA Controller to Processor SCCs**" means the clauses set out at Appendix 1.

2.1.5 "**EEA Processor to Processor SCCs**" means the clauses set out at Appendix 2.

2.1.6 "**GDPR**" means EU General Data Protection Regulation 2016/679;

2.1.7 "**Restricted Transfer**" means a transfer of Personal Data which, subject to the paragraph below, is:

(i) 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**");

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

(iii) 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:

(i) 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

(ii) 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).

2.1.8 "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of Open Text for the Customer pursuant to the Principal Agreement;

2.1.9 "**Standard Contractual Clauses**" means each of the EEA Standard Contractual Clauses and the UK Standard Contractual Clauses;

2.1.10 "**Sub-processor**" means any third party (including any Open Text Affiliate) appointed by or on behalf of Open Text as a sub-contractor to Process Personal Data on behalf of any Customer or Customer Affiliate in connection with the Principal Agreement.

2.1.11 "**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;

2.1.12 "**UK Data Protection Law**" means UK GDPR (as defined in the UK Data Protection Act 2018) and the UK Data Protection Act 2018;

2.1.13 "**UK Controller to Processor SCCs**" means the UK International Data Transfer Addendum which is made up of the provisions set out in Appendix 6 incorporating the EEA Standard Contractual Clauses to the extent it applies in respect of the transfer of Personal Data from a Controller to a Processor.

2.1.14 "**UK Processor to Processor SCCs**" means the UK International Data Transfer Addendum which is made up of the provisions set out in Appendix 6 incorporating the EEA Standard Contractual Clauses the extent it applies in respect of the transfer of Personal Data from a Processor to a Processor; and

2.1.15 "**UK Standard Contractual Clauses**" means the UK Controller to Processor SCCs and UK Processor to Processor SCCs (each as amended, updated or replaced from time to time).

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 meanings as in the GDPR. The terms "**data exporter**" and "**data importer**" have the meanings set out in the applicable Standard Contractual Clauses. "including" shall mean including without limitation.

Part B: Data Processing Obligations

3 **Controller and Processor of Personal Data, Appointment of Processor and Purpose of Processing**

3.1 Open Text will comply with all applicable requirements of the Data Protection Legislation and expects Customer to also comply with Data Protection Legislation.

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

3.3 Appendix 3 of this DPA sets out the scope, nature and purpose of Processing by Open Text, the duration of the Processing and the types of Personal Data and categories of Data Subjects.

4 **Open Text's obligations with respect to the Customer**

4.1 Open Text will, in relation to any Personal Data it will be Processing under the Principal Agreement and this DPA:

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

4.1.2 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;

4.1.3 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

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

4.2 Customer agrees that the Principal Agreement (including this DPA) are its complete documented instructions to Open Text for the Processing of Personal Data. Additional instructions, if any, require prior written agreement between the Parties. Where in the opinion of Open Text an instruction from the

Customer infringes Data Protection Legislation, it shall inform the Customer thereof (but such communication shall not constitute legal advice by Open Text). However, such obligation shall not relieve the Customer from its own responsibility for compliance with Data Protection Legislation.

4.3 Where Open Text 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, Open Text 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.

5 Sub-processing

5.1 Customer provides Open Text a general authorization to engage Sub-processors. Sub-processors may include: (i) Open Text's global Affiliate companies as exist from time to time (and their vendors); and/or (ii) any of the sub-contractors that Open Text 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.

5.2 Open Text shall Inform the Customer at least 14 days before Open Text appoints a new or replacement Sub-processor to give the Customer opportunity to reasonably object to the changes. Open Text must receive the notice of objection in writing from the Customer within 14 days of Open Text 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 Open Text global Affiliate company.

5.3 The Parties agree that the Customer's right to be object shall be as set out in this clause 5.3 and clause 5.4. Any objection raised by the Customer pursuant to clause 5.2 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.

5.4 If Customer has a reasonable and legitimate reason to object to the new Sub-processor pursuant to clause 5.3, and Open Text 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 Open Text no later than 30 days from the date that Open Text receives the Customer's notice of objection and such termination shall take effect no later than 90 days following Open Text'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 clause 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).

5.5 Open Text 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.

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

6 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.

7 Exercise of Data Subjects' Rights

7.1 Taking into account the nature of the Processing, Open Text 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.

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

8 Notification of Personal Data Breach

8.1 Open Text shall notify the Customer of a Personal Data Breach without undue delay by email to a Customer email address on file with Open Text, 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.

8.2 If available and taking into account the nature of the Processing, the notification in accordance with clause 8.1 shall at least:

8.2.1 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;

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

8.2.3 describe the likely consequences of the Personal Data Breach;

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

8.3 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.

8.4 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.

9 Assistance lent by Open Text to the Customer regarding Compliance with Customer's Obligations under the Data Protection Legislation

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

9.1.1 in carrying out data protection impact assessments; or

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

10 Security Measures

10.1 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 Open Text shall both be responsible to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

10.2 Open Text agrees to implement the technical and organizational measures set out in Appendix 5 in respect of the Services.

10.3 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 Open Text access to systems or Personal Data to only where essential for the performance of Services. Where Open Text 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 Open Text 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.

11 Data Return or Destruction

Where Open Text has stored Personal Data as part of the Services: at the end of the Service(s) upon the Customer's written instruction, Open Text 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. Open Text may charge a fee for any data return services.

12 The Data Protection Officer

Open Text has designated a data protection officer in accordance with Data Protection Legislation. Open Text's data protection officer can be contacted by email via DPO@opentext.com.

13 Inspections and Audits

13.1 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 Clause 13.

13.2 Upon written request from Customer Open Text 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 Open Text relating to the Personal Data is in compliance with its obligations under this DPA.

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

13.4 Customer may conduct an on-site inspection at Open Text's premise either by itself or by an independent third-party auditor (which shall not include a competitor of Open Text) where the information under Clause 13.2 and 13.3 has failed to verify compliance by Open Text of its obligations under this DPA or such an inspection is formally required by the Supervisory Authority.

13.5 General Procedure: The following shall apply to each of Clauses 13.2, 13.3 and 13.4.

13.5.1 Unless otherwise mandated by a Supervisory Authority, the Customer shall (a) give Open Text at least 30 days' prior written notice of its intention to conduct an audit, including inspection, under this Clause 13; and (b) agree with Open Text the frequency and duration of these, which shall not extend beyond two consecutive business days and not be more than once per contract year.

13.5.2 Any audit, including inspections, must be conducted during local business hours, not unreasonably disrupt Open Text business operations and not burden the provision of services by Open Text to its customers. Customer shall limit these to remote audits or meetings with senior representatives of Open Text 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 Open Text's relevant policies and procedures.

13.5.3 Conditions of confidentiality and the scope of an audit, including inspection, shall be agreed in advance between Open Text and Customer. Customer shall provide Open Text the results of any audit, including inspection. Customer shall bear all costs and expenses related to the inspections or audits.

14 **Customer Information and related Restrictions**

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

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

14.3 Open Text will deal without undue delay with reasonable inquiries from the Customer about the Processing of Personal Data in accordance with this DPA.

Part C: International Transfers

15 **International Transfers**

15.1 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 Open Text or its Sub-processors. The transfer to Other Countries shall be in accordance with Data Protection Legislation (to the extent it applies).

15.2 The Parties shall have in place a Transfer Mechanism in respect of any Restricted Transfer.

15.2.1 In the event of an EEA Restricted Transfer where Personal Data is transferred from Customer as data exporter acting as a Controller to Open Text as data importer acting as a Processor, the Parties shall, as part of this DPA, comply with the EEA Controller to Processor SCCs.

15.2.2 In the event of an EEA Restricted Transfer where Personal Data is transferred from Customer as data exporter acting as a Processor to Open Text as data importer acting as a Processor, the Parties shall, as part of this DPA, comply with the EEA Processor to Processor SCCs.

15.3 In the event of a UK Restricted Transfer, where Personal Data is transferred from Customer as data exporter acting as a Controller to Open Text as data importer acting as a Processor, the Parties shall, as part of this DPA, comply with the UK Controller to Processor SCCs.

15.4 In the event of an UK Restricted Transfer where Personal Data is transferred from Customer as data exporter acting as a Processor to Open Text as data importer acting as a Processor, the Parties shall, as part of this DPA, comply with the UK Processor to Processor SCCs.

15.5 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.

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

15.7 Where pursuant to the Standard Contractual Clauses Open Text 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.

Part D: Final Provisions

16 Execution of this DPA

16.1 Where requested by Customer, Open Text and Customer shall execute this DPA in two counterparts. However, this DPA shall also be valid without signature and bind Open Text, subject to and under the condition of Customer fully complying with Data Protection Legislation.

16.2 The Parties agree that with respect to the period on and after the date that this DPA comes into effect between the Parties, this DPA shall replace and supersede any existing data processing addendum, attachment, exhibit or standard contractual clauses that Customer and Open Text may have previously entered into in connection with the Services.

_____ **(Open Text)** Name: Title: Date: Address:	_____ **(Customer)** Name: Title: Date: Address:

APPENDIX 1

EEA CONTROLLER TO PROCESSOR CLAUSES

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

[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.

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(b), 8.9(a), (c), (d) and (e);

(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 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,

[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.

thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

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

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

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

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

Clause 10

Data subject rights

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.

(a) 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.

(b) 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.

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

(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.

(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:

[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.

(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.

ANNEXES OF APPENDIX 1

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 Appendix 4 for activities relevant to the data transferred under these Clauses.

B DESCRIPTION OF TRANSFER

See Appendix 4 of this 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 Appendix 5 of this DPA.

APPENDIX 2

EEA PROCESSOR TO PROCESSOR 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')

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

[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.

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

(i) 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.

(ii) 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.

(iii) 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.

(iv) 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 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

(v) 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.

(vi) 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

[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.

authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(vii) 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.

(viii) 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 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;

(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

[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.

(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.

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

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

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

Clause 10

Data subject rights

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.

(a) 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.

(b) 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.

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;[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.

(d) 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.

(e) 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.

(f) 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.

ANNEXES OF APPENDIX 2

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 Appendix 4 for activities relevant to the data transferred under these Clauses.

B DESCRIPTION OF TRANSFER

See Appendix 4 of this 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 Appendix 5 of this DPA.

APPENDIX 3

DETAILS OF PROCESSING OF CUSTOMER PERSONAL DATA

Subject matter and duration of the Processing of Personal Data

See Appendix 4.

The nature and purpose of the Processing of Personal Data

See Appendix 4.

The types of Personal Data to be processed

See Appendix 4.

Special categories of data (if appropriate)

See Appendix 4.

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

See Appendix 4.

APPENDIX 4

DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Unless provided otherwise by the Customer, Data Subjects may include Customer employees, contractors, business partners or other individuals having Personal Data stored, transmitted to, made available to, accessed or otherwise processed by Open Text.

Categories of personal data transferred

Customer determines the categories of Personal Data which are processed by Open Text 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 Open Text 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. Open Text disclaims all liabilities in relation to the selection of data performed by Customer 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

Open Text offers Services to the Customer. Open Text requires to process Personal Data to deliver the Services to the Customer.

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) execution of instructions of Customer in accordance with the Principal Agreement and DPA.

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

In respect of the Standard Contractual Clauses, transfers to Sub-processors shall be on the same basis as set out in the DPA.

APPENDIX 5

TECHNICAL AND ORGANIZATIONAL MEASURES

This Appendix 5 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 centers.

Data center facilities are designed to physically protect equipment and other critical resources from unauthorized access and environmental hazards. The Open Text data centers 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 centers 24 hours a day x 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 center and areas within the data center to restrict access. Personnel must pass an area where they are observed by security company personnel and access to the data center through a circle lock / mantrap to prevent tailgating

(c) Within the data center 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 onsite with issuance registration

(e) Emergency exterior door opening triggers an audible alarm when opened

(f) Third party visitors and deliveries must be pre-announced, access approved by listed approvers and visitors are escorted in the data center

(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 center 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 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 user's 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, 1 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 that data is 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 centers or facilities. Security measures which 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. Also, 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 for fulfil job functions.

Change Control

In addition, all system changes must be recorded, verified, tested and approved following a change management process which 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 center facilities are designed to physically protect equipment and other critical resources from unauthorized access and environmental hazards. Data centers 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 pro-actively monitored 24 hours a day and 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 6

UK INTERNATIONAL DATA TRANSFER ADDENDUM
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 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.	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.
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	×	×	×			
2	✓	✓	×	General	14 days	
3	✓	✓	×	General	14 days	
4	×	×	×			×

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 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 Appendix 4 of this DPA.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Appendix 5 of this DPA.
Annex III: List of Sub processors (Modules 2 and 3 only): See Clause 5.1 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.

opentext™

Schedule – OpenText™ Core Content

This schedule is ancillary to the OpenText Core Applications & Services Supplemental Terms to the OpenText Cloud General Terms & Conditions referenced on the Order.

Definitions

"S/4HANA Cloud (Essentials Editions)" means the multi-tenant cloud version of SAP's S/4HANA offering.

"M365" means the Microsoft office suite including apps like Word, PowerPoint, Excel and Teams.

"Salesforce" means the online customer relationship management services provided to the Customer by salesforce.com marketed as 'Sales Cloud', 'Service Cloud' or 'Financial Services Cloud' but excluding third-party applications and services.

Core Cloud Service	**OpenText Core Content**
Description	OpenText Core Content Service is a cloud-based content management platform, including capabilities for document management, business workspaces, integration into business applications, full text search and retention management.
Provisioned Tenants	One production tenant One non-production tenant
Available SKU's / Product Names	Core Content (SKU: 1000056093) – Standard Named Users Core Content Buy-Ahead Storage (SKU: 1000056263) - Gigabytes
Available Data Center Regions	North America EMEA
Unit of Measure	Access and use of the Core Content Cloud Services is measured as follows: 1) Standard Named User. For each Subscription SKU identified with a Standard Named User unit of measure, Customer must purchase and allocate one Standard Named User for each Authorized User of the production tenant Cloud Service (regardless of whether the Authorized User accesses or uses the Core Cloud Service) ("Standard Named User Subscription"). A Standard Named User Subscription cannot be shared, re-allocated, or exchanged between individuals, except that Standard Named User Subscription may be reallocated to another individual if the original individual is no longer employed by Customer or has been permanently assigned to a new role that does not require access to the Core Cloud Service. To re-allocate such Standard Named User Subscription to another individual, the original individual's user account must first be deleted from the system. Until the user's account has been deleted from the system, a Standard Named User Subscription is required even if the user is no longer an employee or contractor of Customer. For avoidance of doubt, Customer must purchase and allocate one Standard Named for any user account that has been disabled, regardless of whether the disabled account is accessed or used. When Customer allocates a Standard Named User Subscription to an individual, Customer must also assign unique login credentials to the individual for the purpose of allowing the individual to access the Core Cloud Service. Customer must purchase an additional Standard Named User Subscription for each additional login and password combination assigned to an individual. Multiplexing does not reduce the number of Standard Named User Subscriptions required. If Customer utilizes Multiplexing, Customer must maintain a permanent record of user activity sufficient to quantify the users of the Core Cloud Service and in advance of access or use, Customer must purchase sufficient Standard Named Users for all users accessing or authorized to access the Core Cloud Service through Multiplexing. "Multiplexing" means using the Core Cloud Services in a manner that reduces the ability to distinguish or detect the

opentext™

Core Cloud Service	OpenText Core Content
	number of individuals directly or indirectly accessing or utilizing the Core Cloud Service (sometimes called "multiplexing" or "pooling" software or hardware). 2) Gigabytes. For each SKU identified with a Gigabytes unit of measure, Gigabytes means the total aggregate amount of storage (in gigabytes) across all of the Customer's tenants that is used to store Content in the Cloud Service.
Overage Items	Access and use of Core Content Cloud Services and the Client Side Software components detailed below is limited to the quantities and Unit of Measure stated in the Order and subject to the terms described herein. If such limitations are exceeded, Customer shall be invoiced for the requisite fees for the excess usage.
Client Side Software integration pre-requisites	Client Side Software integration components that facilitate the integration between Core Content and business applications are included in the Service and available to download if the customer chooses to install and configure (all required details to be found on MySupport). Installation and configuration services of these components are not included in the Core Cloud Service; Customer may complete installation and configuration on their own or elect to purchase additional professional services from OpenText to assist. Customer who has an active S/4HANA Cloud (Essentials Editions) service can: • Configure and synchronize S/4HANA business objects and Core Content business workspaces. • Integrate into S/4HANA Cloud user interface (only for supported S/4HANA business objects, it requires SAP Cloud Platform integration component). Customer who has an active M365 tenant can: • Integrate with Office Online for viewing and editing of Microsoft Office formats and integrate with Microsoft Teams for content sharing and collaboration. Customer who has an active Salesforce subscription can: • Configure and synchronize Salesforce business objects and Core Content business workspaces. • Display content into the Salesforce UI via standard business objects.
Client Side Software integration components	The following Client Side Software components are available for download and included in this Core Cloud Service. 1) OpenText Core Content S/4HANA Cloud (Essentials Editions) a. Customer may utilize this component up to the lesser of (i) the number of Core Content (1000056093) Standard Named Users subscribed; or (ii) the number of users subscribed to S/4HANA Essential. 2) OpenText Core Content M365 Integration a. Customer may utilize this component up to the lesser of (i) the number of Core Content (1000056093) Standard Named Users subscribed; or (ii) the number of users subscribed to M365 3) OpenText Core Content Salesforce Integration a. As a prerequisite to receiving this Client Side Software component, Customer must provide OpenText the unique ID of their production Salesforce system (the "**Customer Salesforce Org ID**"). Failure to provide OpenText the Customer Salesforce Org ID will prevent Customer from using this component.

opentext™

Core Cloud Service	OpenText Core Content
	b. This integration is facilitated by download of the OpenText Core Content application from the AppExchange (the online directory of applications that interoperate with Salesforce). c. Service notices may be provided by notification directly through the Customers' Salesforce system user interface. d. Customer may utilize this component up to the lesser of (i) the number of Core Content (1000056093) Standard Named Users subscribed; or (ii) the number of users subscribed to Salesforce. e. Each party agrees that Confidential Information may be disclosed to salesforce.com Inc. or its affiliates in connection with the Customer's Salesforce usage within the OpenText Core Content Service.
Client Side Software Specific Terms	Verification: During the term of the Order and for 24 months after, Customer will maintain electronic and other records sufficient for OpenText to confirm that Customer's use of the Client Side Software has complied with the applicable Order and this schedule. Customer will promptly and accurately complete and return (within 30 days of OpenText request) any self-audit questionnaires, along with a certification by an authorized representative of Customer confirming that Customer's responses to the questionnaire accurately and fully reflect Customer's usage of the Client Side Software components. OpenText may once every six months audit Customer's records and computer systems (including servers, databases, and all other applicable software and hardware) to ensure Customer has complied with the Order and this schedule. Customer shall cooperate with OpenText and promptly and accurately respond to any reports requested by OpenText and provide a certification by an authorized representative of Customer confirming that information provided by Customer accurately reflects Customer's usage of the Client Side Software. If Customer is not in compliance with the terms and conditions governing the Client Side Software, Customer will be deemed to have acquired additional subscriptions at OpenText's then-current list price to bring Customer into compliance, and Customer must immediately pay the applicable fees and taxes for the period during which Customer was not in compliance with the Order and this schedule
Application Specific Terms	1) For Core Content (1000056093): a. Business Unlimited storage is included; where "Business Unlimited" means unlimited use of storage, up to the Storage Quota (as defined in the subsequent sentence), to manage Content for Customer's business processes (for example: PDFs, Office Documents, email, pictures and movies) by Standard Named Users. "Storage Quota" means the total maximum storage amount allowed for use and access by the Customer across the Customer's production and non-production tenants, calculated at **100GB per Standard Named User** purchased. For example, a purchase of 100 Standard Named Users allows a Storage Quota of 10TB. 10TB is approximately equivalent to 100 million PDFs (100KB average size) or 20 million Office documents (500KB average size). A Standard Named User's use of storage is not limited to 100GB; a Standard Named User may exceed 100GB of storage use, provided that the Storage Quota is not exceeded. Use of additional storage over the Storage Quota will require Customer to either: (i) pay overage fees for storage in arrears; or (ii) purchase additional Storage Quota in advance. b. For each production tenant purchased under this SKU, Customer will have access and use to one (1) non-production tenant that shall be used solely for test or development purposes. Use of the non-production tenant for any other purpose, including for production purposes, requires Customer to purchase an additional subscription to this SKU. The number of Standard Named Users who may access and use the non-production tenant is limited to 10% of the Standard Named Users purchased for the production tenant. The included storage

Core Cloud Service	OpenText Core Content
	amount for the non-production tenant is calculated at 10GB of storage for each Standard Named User allowed for use or access in the non-production tenant. 2) Core Content Buy-Ahead Storage (1000056263) is an add-on SKU, where the Customer must also be simultaneously subscribed to Core Content (1000056093). The quantity specified in the Order equals the number of 500 Gigabyte blocks of storage being added to the Customer's production tenant only. Purchase of this SKU must be co-termed with the Customer's subscription to Core Content (1000056093).