Micro Focus Supplier Data Privacy and Protection Agreement (DPA) (as at 28 March 2023)

This Supplier DPA and its annexes form part of the applicable purchase agreement/order between Micro Focus (acting on its own behalf and its Affiliates) (Micro Focus) and Supplier ("Contract"). Capitalized terms not specifically defined herein shall have the meaning set forth in the Contract. This DPA shall be considered an Exhibit/Schedule under the Contract and shall be deemed to amend (as applicable) and form part of the Contract by and between Micro Focus and Supplier.

1 DEFINITIONS

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

1.1 **"Affiliate"** means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with a party, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of management and the policies of an entity, whether through ownership of voting securities, by contract or otherwise.

1.2 "**Data Protection Legislation"** means data protection and privacy laws including, without limitation, (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 Contract.

1.3 **"EEA Controller to Processor SCCs"** means the standard contractual clauses between controllers and processors, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, which are set out in this DPA as they are to apply to this DPA (as amended, updated or replaced from time to time).

1.4 **"EEA Processor to Processor SCCs"** means the standard contractual clauses between processors and processors, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, which are set out in this DPA as they are to apply to this DPA (as amended, updated or replaced from time to time).

1.5 **"EEA Standard Contractual Clauses"** means the EEA Controller to Processor SCCs and EEA Processor to Processor SCCs

1.6 **"GDPR"** means EU (European Union) General Data Protection Regulation 2016/679.

1.7 **"Other Standard Contractual Clauses"** means for Personal Data subject to Data Protection Legislation other than (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, the standard contractual provisions or model clauses approved by the corresponding data protection authority in order to lawfully transfer Personal Data internationally under applicable Data Protection Legislation, as may be amended, updated or superseded from time to time.

1.8 **"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 Law if a Transfer Mechanism is applicable to that transfer ("UK Restricted Transfer");

(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"); and/or

(iv) from an exporter subject to Data Protection Legislation (other than those cited in (i), (ii) and (iii) above) which is only permitted under applicable Data Protection Legislation if Other Standard Contractual Clauses are applicable to that transfer ("Other Restricted Transfer").

Transfers of Personal Data will not be considered a Restricted Transfer where: (v) the jurisdiction to which the personal data is transferred has been approved by the European Commission pursuant to Article 25(6) of the EC Directive 95/46 or Article 45 of the GDPR or, as applicable, an equivalent provision under UK or Swiss Data Protection Legislation, as ensuring an adequate level of protection for the processing of personal data; or (vi) the transfer falls within the terms of a derogation as set out in Article 49 of the GDPR, equivalent under Swiss Data Protection Legislation or the UK GDPR (as applicable).

1.9 **"Services"** means the services and other activities to be supplied or carried out by or on behalf of Supplier for Micro Focus (or Micro Focus's customer) pursuant to the Contract.

1.10 **"Standard Contractual Clauses"** means each of the EEA Standard Contractual Clauses, the UK Standard Contractual Clauses and the Other Standard Contractual Clauses.

1.11 **"Sub-processor"** means any third party (including, without limitation, any Supplier Affiliate) appointed by or on behalf of Supplier to Process Personal Data on behalf of Micro Focus or Micro Focus Affiliate in connection with the Contract.

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

1.13 **"UK Data Protection Law"** means UK GDPR and the Data Protection Act 2018

1.14 **"UK GDPR"** has the meaning defined in The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019.

1.15 **"UK Controller to Processor SCCs"** means the UK International Data Transfer Addendum which is set out in this DPA as it is to apply to this DPA, and may be amended, updated or replaced from time to time, 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.

1.16 **"UK Processor to Processor SCCs"** means the UK International Data Transfer Addendum which is set out in this DPA as it is to apply to this DPA, and may be amended, updated or replaced from time to time, incorporating the EEA Standard Contractual Clauses the extent it applies in respect of the transfer of Personal Data from a Processor to a Processor.

1.17 **"UK Standard Contractual Clauses"** means the UK Controller to Processor SCCs and UK Processor to Processor SCCs.

1.18 The terms **“Controller”**, **"Data Subject"**, **"Personal Data"**, **"Personal Data Breach"**, **"Processing"**, **“Processor”** and **"Supervisory Authority"** shall have the same meaning as in the GDPR (or, where the relevant processing is subject to alternative Data Protection Legislation, the defined term or concept set out in such application Data Protection Legislation with the closest equivalent meaning to that given under the GDPR).

2 DATA PROTECTION

2.1 Each party will comply with all applicable requirements of the Data Protection Legislation. This DPA is in addition to, and does not relieve, remove, or replace either party’s obligations under the Data Protection Legislation.

2.2 If Supplier determines the purposes and means of any Processing of Micro Focus’s Personal Data, Supplier becomes the Controller for such Processing and is, consequently, solely responsible for the lawfulness of such Processing by Supplier as Controller under applicable Data Protection Legislation. For the avoidance of doubt, Supplier is only permitted to process Personal Data for the purposes set out in clause.

2.3 Appendix B sets out details of the subject matter, nature and purpose of processing, type of personal data and categories of data subject. The duration of processing is the duration of the Contract.

2.4 To the extent that Supplier currently has, has had, or will have access or potential access to Personal Data of Micro Focus and/or its customers or has or will generate, process, store or transmit Personal Data in providing the Services, in relation to any Personal Data processed under the Contract and this DPA, Supplier agrees to:

2.4.1 process, use and maintain Personal Data for Micro Focus and/or its customers only in accordance with Micro Focus's documented written instructions and the Contract (together with this DPA) solely for the purposes of performing its responsibilities and obligations under the Contract unless required to do so by (i) in respect of Personal Data subject to GDPR, EU or Member State Law; (ii) in respect of Personal Data subject to UK Data Protection Legislation, laws applicable in the United Kingdom; and (iii) in respect of Personal Data subject to other Data Protection Legislation (excluding GDPR and UK Data Protection Law), applicable laws, provided that the Supplier shall notify Micro Focus of that legal requirement before Processing. The Supplier shall make no other use of Personal Data other than for the provision of the Services to Micro Focus. Supplier represents and warrants that nothing would prevent it from fulfilling such obligations;

2.4.2 where in the opinion of Supplier an instruction from Micro Focus infringes Data Protection Legislation, it shall inform Micro Focus thereof (but such communication shall not constitute legal advice by Supplier). However, such obligation shall not relieve Supplier from its own responsibility for compliance with Data Protection Legislation;

2.4.3 neither (a) sell or disclose the Personal Data to any third party for the commercial benefit of Supplier or any third party; nor (b) retain, use, disclose or otherwise Process the Personal Data outside of the direct business relationship between the Parties. Supplier certifies that it understands and will comply with all restrictions placed on its Processing of the Personal Data;

2.4.4 take appropriate technical and organizational measures to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access or use, and against all other unlawful forms of Processing. The Supplier shall notify Micro Focus without undue delay in case of any changes to the technical and organizational matters which affect the Personal Data or that would otherwise reduce the level of protection of Personal Data;

2.4.5 ensure that only personnel who need to have access to Personal Data for provision of the Services are granted access to such Personal Data and only for the purposes of the performance of the Services and inform all personnel of the confidential nature of the Personal Data and ensure personnel are subject to appropriate obligations of confidentiality and have received appropriate training on their responsibilities;

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

2.4.7 where a Data Subject submits a request to the Supplier to exercise their rights, the Supplier shall forward these requests by email to Micro Focus at privacy@microfocus.com or such other contact details notified by Micro Focus's Privacy Team to Supplier in writing from time to time. The Supplier shall not respond to a Data Subject request unless and to the extent instructed by Micro Focus to do so;

2.4.8 without undue delay (but in any case within 24 hours) notify Micro Focus in writing if it becomes aware of (i) any accidental or unauthorized access to Personal Data, (ii) any actual or potential Personal Data Breach or breach of this DPA and / or Data Protection Legislation, (iii) any disclosure or request for disclosure of Personal Data to a third party (except for disclosure to an approved Sub-processor in accordance with Clause 2.4.10) and (iv) any request for disclosure or inquiry from a third party (including, without limitation, a public authority) concerning the Personal Data; and, (v) any change in applicable law that would render Supplier unable to comply with this DPA. All such notices shall be directed to privacyincidents@opentext.com in addition to that specified in any notice procedures set forth in the Contract;

2.4.9 If available and taking into account the nature of the Processing, the notification in accordance with clause 2.4.8 (i) and/or (ii) above shall at least:

(a) describe the nature of the Personal Data Breach including without limitation and where possible, the categories and approximate number of Data Subjects concerned, and the categories and approximate number of Personal Data records concerned;

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

(c) describe the likely consequences of the Personal Data Breach; and

(d) describe the measures taken or proposed to be taken by the Supplier to address the Personal Data Breach, including without limitation, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide the information at the same time or becomes available later, the information may be provided in phases without undue further delay;

2.4.10 not subcontract any of its Processing operations performed on behalf of Micro Focus or any Micro Focus Affiliate without the prior written consent of Micro Focus. The Supplier shall submit the request for prior written consent at least 60 days prior to the engagement of the sub-processor, together with the information necessary to enable Micro Focus to decide whether to provide its prior written consent. Micro Focus has provided consent to those Sub-processors set out at Appendix D. Where Supplier subcontracts its obligations, it shall do so only by way of a written agreement with the Sub-processor which imposes the same obligations on the Sub-processor as are imposed on Supplier under this DPA. Supplier confirms that it has entered or (as the case may be) will enter into a written agreement with its Sub-processors incorporating terms which are substantially similar to those set out in this DPA. Supplier shall remain fully liable to Micro Focus for all acts or omissions of any Sub-processor;

2.4.11 not make a transfer of Personal Data (including, without limitation any Restricted Transfer of Personal Data by the Supplier to any Sub-processor), and procure that Sub-processors do not make a transfer of Personal Data, without the prior written consent of Micro Focus and provided always that such transfer and/or Restricted Transfer is compliant with Data Protection Legislation including, without limitation Standard Contractual Clauses entered into between the Supplier and relevant Sub-processor. The Supplier confirms that it has entered into Standard Contractual Clauses and/or Other Standard Contractual Clauses with all Sub-processors where there is a Restricted Transfer. Supplier shall provide copies of the applicable Transfer Mechanism in place with Sub-processors promptly if requested by Micro Focus (provided that Supplier may redact commercially sensitive and confidential information);

2.4.12 within five (5) business days of receipt of a written request from Micro Focus:

(a) provide Micro Focus (or Micro Focus's customers where applicable) with reasonable access to its personnel, premises, facilities and Sub-processors to enable Micro Focus to conduct an on-site inspection audit;

(b) authorise Micro Focus to make confidential copies of any materials including, without limitation, any records and information required to be obtained and maintained under the Contract, this DPA and Data Protection Legislation which are relevant to assessing compliance with the Contract and DPA and, where applicable, to share such copies with Micro Focus's customers;

(c) provide evidence of Supplier's relevant policies and other related documents to verify that Supplier is complying with its obligations under this DPA and, where applicable, to share such copies with Micro Focus's customers; and

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

2.4.13 Any on site audit under Clauses 2.4.12(a) ("On Site Audit") shall be conducted during ordinary business hours on business days and shall not interfere unreasonably with Supplier's ordinary business. If the results of an On Site Audit or other audit of information provided pursuant to Clause 2.4.12 (together an "Audit") show that Supplier is not complying with the Contract and/or DPA, then Supplier must ensure prompt remedy of the non-compliance and comply with Micro Focus's reasonable directions to remedy the non-compliance, including without limitation directions as to timing. Any Audit shall be conducted, and all information to be provided pursuant to this clause shall be provided, at the cost of the Supplier;

2.4.14 On termination of the Contract, return to Micro Focus or permanently delete all copies of such Personal Data, as directed by Micro Focus, and certify compliance with this obligation in writing to Micro Focus. Such certification of compliance to be signed by a signing officer of Supplier; and

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

2.5 Supplier agrees to comply with the terms of Appendix A: 'Technical and Operational Measures', which form part of the Contract and this DPA.

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

2.7 **International transfers**

2.7.1 The Parties shall have in place a Transfer Mechanism in respect of any Restricted Transfer between the Parties and shall comply with Appendix C if there is a Restricted Transfer.

2.7.2 In the event of an EEA Restricted Transfer or Swiss Restricted Transfer where Personal Data is transferred from Micro Focus as data exporter acting as a Controller to Supplier as data importer acting as a Processor, the Parties shall, as part of this DPA, comply with the EEA Controller to Processor SCCs, which are hereby incorporated into this DPA.

2.7.3 In the event of an EEA Restricted Transfer or Swiss Restricted Transfer where Personal Data is transferred from Micro Focus as data exporter acting as a Processor to Supplier as data importer acting as a Processor, the Parties shall, as part of this DPA, comply with the EEA Processor to Processor SCCs, which are hereby incorporated into this DPA.

2.7.4 In the event of a UK Restricted Transfer, the Parties shall, as part of this DPA, comply with the UK Standard Contractual Clauses, which are hereby incorporated into this DPA.

2.7.5 In the event of an Other Restricted Transfer, the Parties shall, as part of this DPA, comply with the Other Standard Contractual Clauses, which are hereby incorporated into this DPA. To the extent applicable, the information set out in the Appendices of the EEA Standard Contractual Clauses shall apply (where relevant) in respect of the Other Standard Contractual Clauses.

2.7.6 For the purposes of the EEA Standard Contractual Clauses, Annex 1 (Description of Transfer) shall be deemed to incorporate the information set out at Appendix E to this DPA; Annex 2 (Description of Technical and Organisational measures) shall be deemed to incorporate the terms set forth in Appendix A to this DPA (Technical and Organisational measures) and Annex 3 (List of Sub-processors) shall be deemed to incorporate the information set forth in Appendix D to this DPA.

2.7.7 If there is a conflict between the provisions of the Standard Contractual Clauses and this DPA the Standard Contractual Clauses shall prevail. Micro Focus may at its discretion, utilise another appropriate cross-border transfer mechanism approved by an appropriate data protection authority or the European Commission (as applicable) which has been adopted by and agreed to by Micro Focus.

2.7.8 Where the Standard Contractual Clauses apply between Micro Focus and Supplier, if the Supplier has factually disappeared, ceased to exist in law or has become insolvent, Micro Focus's customer (as a third-party beneficiary right) shall have the right to terminate the relevant portion of the agreement with the Supplier pertaining to that customer and to instruct the Supplier to erase or return its Personal Data.

2.8 Where any replacement of , or amendment to, the Standard Contractual Clauses is approved by the competent authority/ies or governmental body/ies (including, without limitation, a supervisory authority or the European Commission or a UK Government Department) (**"New Solution"**), the New Solution will be deemed incorporated into the DPA and Contract and take effect and be binding on the parties from the date of such approval by the applicable competent authority or governmental body or, if later, the end of any grace period applicable to the New Solution. In the event reasonably required by Micro Focus or Supplier or where required by applicable Data Protection Legislation or on request by the competent authority/ies or governmental body/ies, Micro Focus and Supplier shall enter into signed copies of the New Solution with details of processing as set out in, or substantially similar to, those set out in the Standard Contractual Clauses.

2.9 **Conflict**

2.9.1 If there is an inconsistency between any of the provisions of the Standard Contractual Clauses, this DPA and the provisions of the Contract in relation to the Processing of Personal Data, the provisions of the Standard Contractual Clauses shall prevail over the DPA and Contract, and this DPA shall prevail over the Contract.

2.10 Other provisions

2.10.1 The Parties agree that this DPA shall replace and supersede any existing data processing addendum, attachment, exhibit or standard contractual clauses that Supplier and Micro Focus may have previously entered into in connection with the Services and shall be effective from 27 December 2022.

2.10.2 The parties confirm that in all other respects, the terms, covenants and conditions of the Contract remain unchanged and in full force and effect, except as modified by this DPA.

It is understood and agreed that all terms and expressions when used in this DPA, unless a contrary intention is expressed herein, have the same meaning as they have in the Contract

APPENDIX A TECHNICAL AND ORGANISATIONAL MEASURES

(IT SECURITY TERMS AND CONDITIONS)

Supplier must comply with the Technical and Organisational Measures (IT Security Terms and Conditions) including, without limitation, its appendices and ensure any subcontractor engaged by the Supplier, also complies with the Technical and Organisational Measures. References to Micro Focus information, Micro Focus data and Micro Focus assets shall be deemed to include Personal Data of Micro Focus and/or its customers or other Personal Data that Supplier has or will generate, process, store or transmit in providing the Services

1. COMPLIANCE

1.1. For all supplier systems used to host, store, process or transmit Micro Focus information, supplier must provide, on an annual basis, an independent audit report (SOC1, SOC2, SOC3, ISO27001, PCI-DSS) that validates the security controls of those systems.

1.2. Additionally, upon request, the supplier must agree to complete an annual information security assessment questionnaire supplied by Micro Focus.

1.3. For all supplier systems used to store, process or transmit Micro Focus information, Micro Focus retains the right to perform a security assessment once a year. Such Assessment may include examination of supplier's relevant facilities and records as may be reasonably required to undertake verification that supplier is complying with its security obligations. The assessment will be conducted at a mutually agreed time with no less than 30 days' advance notification, shall be limited to no more than two (2) business days and shall not unreasonably disrupt Supplier's day-to-day business operations

1.4. In case supplier security and data protection measures do not meet (i) these terms and conditions; (ii) reasonable industry standards and / or (iii) regulatory requirements, supplier and Micro Focus will mutually agree a remediation plan. In case the remediation plan cannot address the findings to the satisfaction of Micro Focus, Micro Focus at its sole discretion may terminate the contract between the parties.

2. ORGANIZATION OF INFORMATION SECURITY

2.1 Supplier must make available upon request, an Information Security point of contact for the duration of the relationship defined in the contract.

2.2 The Information Security point of contact must be responsible to liaise with Micro Focus Information Security Officer on all matters relating to security.

3. HUMAN RESOURCE SECURITY

3.1 Supplier must communicate information security policies to all personnel involved in work on behalf of Micro Focus or with access to Micro Focus data and track that personnel are aware of all security policies.

3.2 Supplier shall regularly train all personnel on information security and privacy matters relevant to the nature of their function. 3.3 Supplier personnel shall be bound by a binding confidentiality agreement before access is granted to any Micro Focus data or assets.

4. PHYSICAL AND ENVIRONMENTAL SECURITY

4.1 Supplier must ensure that all Micro Focus data or assets are stored in a secure location that is protected by industry standard physical protection controls.

5. OPERATIONAL PROCEDURES AND RESPONSIBILITIES

5.1 Supplier must document where Micro Focus's data and assets are hosted and provide Micro Focus with appropriate documentation of the hosting location upon request.

5.2 Supplier must provide to Micro Focus, documentation about their Information Technology processes.

5.3 Supplier must not alter, adapt or modify Micro Focus's systems without Micro Focus approval.

5.4 To the extent applicable to the contract, supplier must adhere to a documented Change Management process that protects changes to Micro Focus data or Micro Focus environments as applicable.

5.5 Supplier must enforce end-point security on assets that connect to Micro Focus infrastructure including encrypted connectivity and anti-virus/anti-malware software

5.6 Supplier must establish a vulnerability detection and management process, and software patch management process on assets accessing Micro Focus data.

5.7 A network vulnerability scan of the in-scope systems must be performed by a reputable third-party provider on annual basis. A summary report of the scan results must be provided to Micro Focus upon request.

5.8 A formal 3rd party application penetration test must be performed by a reputable third-party provider on annual basis, on any internet facing applications being used in the supplier's solution.

5.9 If Micro Focus terminates the contract, supplier must immediately transfer all data and Micro Focus assets to Micro Focus or, at Micro Focus's sole discretion, destroy all data when no longer required. If data is to be destroyed, an approved methodology must be used and the supplier must provide Micro Focus with a certificate of destruction.

5.10 Upon request, supplier must provide Micro Focus with information on roles and responsibilities of individuals that have access to Micro Focus data.

5.11 Upon request, supplier must be able to provide evidence of auditing of any systems accessing Micro Focus data. 5.12 Supplier must not record any conversation conducted with any Micro Focus personnel unless specifically agreed upon by both parties

6. ACCESS CONTROL

6.1 Supplier must maintain an up-to-date list of employees and third parties accessing Micro Focus data, infrastructure, or information at all times.

6.2 Supplier must ensure that a process for termination of personnel including account termination is in place.

6.3 Supplier must ensure and document that access to Micro Focus information is granted according to principle of least privilege.

6.4 Supplier must, on an annual basis or other such frequency, ensure and document that logical accesses are reviewed for need and that unused accounts are removed.

7. INFORMATION SECURITY INCIDENT MANAGEMENT

7.1 Supplier must adhere to a formally documented incident management process.

7.2 Supplier must cooperate with Micro Focus personnel in the diagnosis, investigation and correction of any security incidents or faults that impact Micro Focus data.

7.3 Supplier must notify Micro Focus within 24 hours of suspicion, detection or confirmation of a breach or unauthorized access to Micro Focus information that is hosted/transacted or managed by the supplier.

8. BUSINESS CONTINUITY and DISASTER RECOVERY MANAGEMENT

8.1 Supplier must have business continuity and disaster recovery plans and processes in place to ensure the service for Micro Focus is adequately maintained in the event of any negative impact on the Supplier´s service.

8.2 Supplier will regularly backup Micro Focus data and retain such Micro Focus backup data copies for a minimum of twelve (12) months.

APPENDIX B DETAILS OF THE PROCESSING OF PERSONAL DATA

Subject matter and duration of the Processing of Personal Data

Supplier is processing Personal Data in order to provide Services to Micro Focus and its affiliates under the Contract

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

The nature and purpose of the Processing of Personal Data

Supplier offers Services to Micro Focus

Supplier is required to process Personal Data to deliver the Services to Micro Focus in accordance with the Contract

The Personal Data is subject to the basic processing activities as set out in the Contract which may include, without limitation: (a) use of Personal Data to provide the Services; (b) storage of Personal Data; (c) transmission of personal data; and (d) execution of instructions of Micro Focus in accordance with the Contract.

The types of Personal Data to be processed

Categories of personal data e.g. 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.

Special categories of data (if appropriate)

E.g. racial or ethnic origin, political opinions, religion, trade union membership, genetic data, biometric data, health data or data concerning a data subject's sex life or sexual orientation

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

Data Subjects may include, without limitation, employees of Micro Focus, its affiliates, their partners and/or any customers of the foregoing, customers of Micro Focus's customers, contractors, business partners or other individuals having Personal Data stored, transmitted to, made available to, accessed or otherwise processed by Supplier.

The Supplier agrees to provide additional information as may be requested by Micro Focus from time to time and warrants its accuracy. The Supplier shall enter into other agreements or amendments that may be required as determined by Micro Focus

APPENDIX C INTERNATIONAL DATA EXPORT REQUIREMENTS

1 International Transfers

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

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

The Supplier agrees to provide additional information as may be requested by Micro Focus from time to time and warrants its accuracy. The Supplier shall enter into other agreements or amendments that may be required as determined by Micro Focus

APPENDIX D SUB-PROCESSORS AND LOCATIONS OF PROCESSING

This Exhibit will be completed by the Supplier and provided separately to Micro Focus

The Supplier will process Personal Data in: [insert locations of processing by Supplier including any locations of access to or processing of personal data (such as remote access)]

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

Supplier Group Sub-processors:

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

Third Party Sub-processors

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

APPENDIX E DESCRIPTION OF TRANSFER

1 Data exporter(s):

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

Name	Micro Focus (as in the Contract)
Address	As in the Contract
Contact person's name, position and contact details	Privacy@microfocus.com
Activities relevant to the data transferred under these Clauses: Micro Focus is obtaining Services from the Supplier	
Role	Controller or Processor (as applicable)

2 Data importer(s):

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

Name	Supplier (as in the Contract)
Address	As in the Contract
Contact person's name, position and contact details	As in the Contract
Activities relevant to the data transferred under these Clauses: Micro Focus is obtaining Services from the Supplier	
Role	Processor

3 Categories of data subjects whose personal data is transferred

See Appendix B.

4 Categories of personal data transferred

See Appendix B.

5 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.

See Appendix B for details of special categories of personal data.

Additional safeguards may include, without limitation, specific access restriction, encryption at rest, policies and procedures on handling of the personal data for specific teams

6 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 during the term of the Contract.

7 Nature of the processing

See Appendix B.

8 Purpose(s) of the data transfer and further processing

See Appendix B.

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

See Appendix B.

10 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 Contract.

11 Competent Supervisory authority

Where the data exporter is established in an EU Member State: Netherlands

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: Netherlands

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:

Netherlands

APPENDIX F: EEA Controller to Processor SCCs

PART ONE

These terms form part of the Supplier DPA and is taken as signed and/or accepted with execution and/or acceptance of the Contract.

Swiss Amendments to the EEA Standard Contractual Clauses

With respect to the EEA standard contractual clauses and transfers of Personal Data to which the Swiss Federal Act on Data Protection (as such laws are amended or re-enacted from time to time) ("FADP") applies, these controller to processor standard contractual clauses shall be deemed amended as follows:

a) References to the GDPR shall be understood as references to the FADP;

b) In Annex I.C the "competent supervisory authority" is the Federal Data Protection and Information Commissioner;

c) Where the transfer is subject to both the FADP and the GDPR, the supervisory authority is the Swiss Federal Data Protection and Information Commissioner insofar as the transfer is governed by the FADP, and the supervisory authority is as set forth in the EEA Standard Contractual Clauses insofar as the transfer is governed by the GDPR;

d) Clause 18 (c) shall be interpreted to permit data subjects in Switzerland to bring legal proceedings in Switzerland;

e) The term "personal data" shall include the data of legal entities to the extent such data is protected under the FADP

(Transfer Controller-to-Processor)

FOR THE PURPOSES OF THE EU STANDARD CONTRACTUAL CLAUSES, ANNEX 1 (DESCRIPTION OF TRANSFER), ANNEX 2 (DESCRIPTION OF TECHNICAL AND ORGANISATION MEASURES) AND ANNEX 3 (LIST OF SUB-PROCESSORS) SHALL BE DEEMED TO INCORPORATE THE INFORMATION SET OUT IN THOSE ANNEXES OF THIS DPA AS INDICATED IN THE DPA.

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.

[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

(b) The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other 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 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

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 of 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 […].

iii. Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

iv. Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

v. Clause 13;

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

vii. Clause 16(e);

viii. Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(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.

MODULE TWO: Transfer controller to processor

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 its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in 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

[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.

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

MODULE TWO: Transfer controller to processor

a. SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least sixty (60) days prior to the engagement of the sub-processor, together with the information necessary to enable the

data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

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

MODULE TWO: Transfer controller to processor

a. The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
b. The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
c. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

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

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

MODULE TWO: Transfer controller to processor

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

MODULE TWO: Transfer controller to processor

(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

MODULE TWO: Transfer controller to processor

(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

MODULE TWO: Transfer controller to processor

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

[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.

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

MODULE TWO: Transfer controller to processor

15.1 Notification

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

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

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

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

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

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

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

15.2 Review of legality and data minimisation

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

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

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

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

Clause 17

Governing law

MODULE TWO: Transfer controller to processor

OPTION 1 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 Netherlands

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

(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 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.

APPENDIX G: EEA Processor to Processor SCCs

PART TWO

These terms form part of the Supplier DPA and is taken as signed and/or accepted with execution and/or acceptance of the Contract.

Swiss Amendments to the EEA Standard Contractual Clauses With respect to the EEA standard contractual clauses and transfers of Personal Data to which the Swiss Federal Act on Data Protection (as such laws are amended or re-enacted from time to time) ("FADP") applies, these processor to processor standard contractual clauses shall be deemed amended as follows:

a) References to the GDPR shall be understood as references to the FADP;

b) In Annex I.C the "competent supervisory authority" is the Federal Data Protection and Information Commissioner;

c) Where the transfer is subject to both the FADP and the GDPR, the supervisory authority is the Swiss Federal Data Protection and Information Commissioner insofar as the transfer is governed by the FADP, and the supervisory authority is as set forth in the EEA Standard Contractual Clauses insofar as the transfer is governed by the GDPR;

d) Clause 18 (c) shall be interpreted to permit data subjects in Switzerland to bring legal proceedings in Switzerland;

e) The term "personal data" shall include the data of legal entities to the extent such data is protected under the FADP

(Transfer Processor-to-Processor)

FOR THE PURPOSES OF THE EU STANDARD CONTRACTUAL CLAUSES, ANNEX 1 (DESCRIPTION OF TRANSFER), ANNEX 2 (DESCRIPTION OF TECHNICAL AND ORGANISATION MEASURES) AND ANNEX 3 (LIST OF SUB-PROCESSORS) SHALL BE DEEMED TO INCORPORATE THE INFORMATION SET OUT IN THOSE ANNEXES OF THIS DPA AS INDICATED IN THE DPA

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.

[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 of 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

b. The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other 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 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
   iii. Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
   iv. Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
   v. Clause 13;
   vi. Clause 15.1(c), (d) and (e);

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 […].

vii. Clause 16(e);
viii. Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

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.

MODULE THREE: Transfer processor to processor

8.1 Instructions

a. The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.
b. The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

c. The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.
d. The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter[6].

[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.

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

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

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

b. The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
c. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
d. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

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

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[7] (in the same country as the data importer or in another third country, hereinafter "onward

[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 purposes of these Clauses.

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 of Regulation (EU) 2016/679;
iii. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
iv. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

a. The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.
b. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.
c. The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.
d. The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.
e. Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.
f. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
g. The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

MODULE THREE: Transfer processor to processor

a. OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the prior specific written authorisation of the controller. The data importer shall submit the request for specific authorisation at least sixty (60) days prior to the engagement of the sub-processor, together with the information necessary to enable the controller to decide on the authorisation. It shall inform the data exporter of such

engagement. The list of sub-processors already authorised by the controller can be found in Annex III. The Parties shall keep Annex III up to date.

b. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[8] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
c. The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
d. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
e. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

MODULE THREE: Transfer processor to processor

a. The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.
b. The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
c. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

Clause 11

Redress

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

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.

MODULE THREE: Transfer processor to processor

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:

    ii. 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;

    iii. 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

MODULE THREE: Transfer processor to processor

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

MODULE THREE: Transfer processor to processor

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

MODULE THREE: Transfer processor to processor

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.

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

[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.

not in line with the requirements in paragraph (a). [For Module Three: 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 [for Module Three: , 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 [for Module Three: 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

MODULE THREE: Transfer processor to processor

15.1 Notification

1) 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.

   [For Module Three: The data exporter shall forward the notification to the controller.]

2) 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.
3) 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.). [For Module Three: The data exporter shall forward the information to the controller.]

4) 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.
5) 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.

15.2Review 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. [For Module Three: 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:

    1. 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;
    2. the data importer is in substantial or persistent breach of these Clauses; or
    3. 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 [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

d. [For Modules One, Two and Three: 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.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] 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

MODULE THREE: Transfer processor to processor

OPTION 1: 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 Netherlands

Clause 18

Choice of forum and jurisdiction

MODULE THREE: Transfer processor to processor

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

(f) The Parties agree that those shall be the courts of Netherlands

(g) 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.

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

APPENDIX H: UK INTERNATIONAL DATA TRANSFER ADDENDUM

This is an attachment to and forms part of the Supplier DPA. It is taken as signed and/or accepted with execution and/or acceptance of the Contract.

Part 1: Tables

Table 1: Parties

Start date	Date of the DPA (or the effective date of the DPA, if stated	
The parties	Exporter (who sends the UK Restricted Transfer)	Importer (who receives the UK Restricted Transfer)
The parties' details	See Contract for the following information in respect of each party: name; address; contact person's name, position and contact details	See Contract 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)	NA	NA

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 [X] 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	Clause 11	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	x	x	x			
2	√	√	x	Prior authorisation	60 days	
3	√	√	X	Prior authorisation	60 days	
4	x	x	X			x

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 Agreement and DPA.
Annex 1B: Description of Transfer: See the Description of Transfer Appendix of this DPA.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See the Technical and Organisation Measures Appendix of this DPA.
Annex III: List of Sub processors (Modules 2 and 3 only): See the Sub-processors Appendix of this 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 [x] neither Party