

## MICRO FOCUS SUPPLIER DATA PRIVACY AND PROTECTION VARIATION AGREEMENT

This Supplier Data Privacy and Protection Variation Agreement (“DPP”) and its annexes and any appendices form part of the applicable purchase agreement/order between Micro Focus and Supplier (“Agreement”). Capitalized terms not specifically defined herein shall have the meaning set forth in the Agreement. This DPP shall be considered an Exhibit/Schedule under the Agreement and shall be deemed to amend (as applicable) and form part of the Agreement by and between Micro Focus and Supplier.

### 1. PURPOSE OF THIS DPP & ORDER OF PRECEDENCE.

#### 1.1 Purpose of this DPP is to establish:

1.1.1 Supplier’s obligations in relation to the use and Processing of Data;

1.1.2 Minimum data security standards applicable to the Services and/or Products provided by Supplier; and

1.1.3 Minimum security standards to be met by Supplier in relation to the Processing of Data and access to Micro Focus Information Systems.

#### 1.2 Order of Precedence. Nothing in this DPP relieves Supplier of any obligations under the Agreement, nor shall be deemed a waiver by Micro Focus of any rights or remedies therein. In the event any term or condition in this DPP conflicts with a term or condition of any Agreement with Supplier, then the term or condition of this DPP shall take precedence and control over any conflicting terms in the Agreement. Save as amended by this DPP, all other terms and conditions of the Agreement shall remain in full force and effect.

#### 1.3 Annexes and Appendices to the DPP:

Annex 1 – Data Processing Schedule and additional terms [or]

Annex 1 –Data Processing Schedule and additional terms for transfers outside Europe included if applicable

Annex 2 (as required) – Standard Contractual Clauses for Processors

Appendix 1 – German Federal DPA requirements included if applicable

### 2. AMENDMENTS TO THE AGREEMENT.

The “*Data Processing Schedule*” and additional terms set out below shall supersede and replace any existing Data Protection Provisions in the Agreement.

### 3. GENERAL.

3.1 This DPP may be executed in any number of counterparts, each of which, when executed and delivered, will be an original, and all the counterparts together will constitute one and the same instrument.

3.2 This DPP will be governed by the choice of law and jurisdiction provisions applicable to, and as detailed within, the purchase agreement/order.

**ANNEX 1 to DPP**  
**Supplier Data Privacy and Protection Variation Agreement**  
**ALSO USED FOR TRANSFERS OF PERSONAL DATA OUTSIDE OF EUROPE**  
**Data Processing Schedule**  
*(To be completed by Supplier)*

Categories of Data Subjects (i.e. customer, colleague or both)	
Type of Data Processed (i.e. personal, special categories of data or other)	
Purpose of Data Processing	
Data Retention Period	
Is the Data encrypted (including at transit and at rest)?	
Is the Data protected by technical security measures (e.g. intrusion detection, firewalls, monitoring)?	
Is access to the Data physically and/or technically restricted?	
How frequently is the Data backed – up?	
Do you have documented policies and procedures regulating the use of the Data?	
Are all personnel who have access to the Data subject to confidentiality undertakings? Employees who handle personal data of other employees or customers must receive training in order to ensure that they handle it in accordance with GDPR.	
Has either a Privacy Impact Assessments or Data Protection Impact Assessments been conducted in respect of the system processing the Data? If so, please attach	
Name and Contact Details of your Data Protection Officer (or the person responsible for Data Protection Compliance)	
Please provide details of any Sub-Processors acting on your behalf (to include full company name, registered number and address, and details of the sub-processing arrangements in place)	
(If Applicable) Details of any third party Data Sources	
Location of all Data Processing Centres used by Supplier and/or Sub-Processors	

## 1. Instructions and Details of Processing

- 1.1 Insofar as the Supplier processes Data on behalf of Micro Focus (who shall remain Data Controller), the Supplier shall process the Data only as described in this Schedule or in accordance with Micro Focus' documented instructions as may be updated from time to time by the written agreement of the parties.
- 1.2 The Supplier warrants, represents and undertakes to Micro Focus that the processing it will be undertaking on behalf of Micro Focus is strictly limited to the extent set out in this Schedule. The Supplier shall not undertake any further processing without the prior written consent of Micro Focus, to include but not limited to an updated version of this Schedule.
- 1.3 Without prejudice to clause 1.2, Micro Focus recognises that there may be occasions where the Supplier is required to process the Data in order to comply with applicable laws. In these circumstances, the Supplier is permitted to process the Data for this purpose, but shall (to the extent that it is legally permitted to do so) notify Micro Focus of such processing as soon as possible and within 72 hours.

## 2. Technical and Organisational Measures

- 2.1 The Supplier shall implement and maintain, at its cost and expense, reasonable administrative, physical, technical and organisational measures in relation to the processing of Data by the Supplier:
  - 2.1.1 such that the processing will meet the requirements of data protection laws and ensure the protection of the rights of Data Subjects;
  - 2.1.2 so as to ensure a level of security in respect of Data processed by it is appropriate to the risks that are presented by the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Data transmitted, stored or otherwise processed; and
  - 2.1.3 without prejudice to clause 4.1, insofar as is possible, to assist Micro Focus in the fulfilment of the Micro Focus' obligations to respond to Data Subject Requests relating to Data.
- 2.2 Without prejudice to clause 2.1.2, the Supplier shall, in respect of the Data processed by it under its Agreement with Micro Focus comply with the requirements regarding security of processing set out in data protection laws (as applicable to Data Processors), all relevant Micro Focus Policies/Standards and in the Agreement.

## 3. Using Personnel and other Processors

- 3.1 Other than as set out in this Schedule the Supplier shall not engage another Data Processor for carrying out any processing activities in respect of the Data without Micro Focus' prior written consent. The Supplier shall at all times remain responsible to Micro Focus for all actions of any sub-processors.
- 3.2 The Supplier shall ensure that all Supplier Personnel processing Data are subject to a binding written contractual obligation with the Supplier to keep the Data confidential.
- 3.3 The Supplier shall ensure that access to the Data will be restricted only to those Personnel who need to know / access the Data for the purposes of fulfilling the obligations under the terms of the Agreement.
- 3.4 Without prejudice to any other provision of this Schedule, the Supplier shall ensure that the Supplier Personnel processing Data are reliable and have received adequate training on compliance with the data protection laws applicable to the processing.

## 4. Assistance with Micro Focus' Compliance and Data Subject Rights

- 4.1 The Supplier shall (at no cost or expense to Micro Focus):
  - 4.1.1 immediately record and then refer all Data Subject Requests (which refers to any request made by a Data Subject to exercise their rights and freedoms pursuant to applicable data protection laws) it receives to Micro Focus without undue delay;
  - 4.1.2 provide such information and cooperation and take such action as Micro Focus reasonably requests in relation to a Data Subject Request, within the timescales reasonably required by Micro Focus; and
  - 4.1.3 not respond to any Data Subject Request and/or (unless otherwise required by law) law enforcement authority, compliance agency without Micro Focus' prior written approval.
- 4.2 Without prejudice to clause 1.1, the Supplier shall, at its cost and expense, provide such information, co-operation and other assistance as Micro Focus reasonably requires (taking into account the nature of processing and the information available to the Supplier) to Micro Focus in ensuring compliance with Micro Focus' obligations under data protection laws, including with respect to:
  - 4.2.1 security of processing, includes right to audit upon advance notice;
  - 4.2.2 data protection impact assessments (as such term is defined in Data Protection Laws); and

4.2.3 prior consultation with a relevant supervisory authority regarding high risk processing.

## **5. International Data Transfers**

5.1 The Supplier will not transfer any Data to any country outside the geographic scope of the Agreement or to any international organisation without Micro Focus' prior written consent.

## **6. Records, Information and Audit**

6.1 The Supplier shall maintain complete, accurate and up to date written records of all categories of processing activities carried out on behalf of Micro Focus, containing such information as Micro Focus may reasonably require, including:

6.1.1 the categories of processing carried out on behalf of Micro Focus

6.1.2 where applicable, details of transfers of Data to an International Recipient; and

6.1.3 a general description of the technical and organisational security measures referred to in clause 2.1.

6.2 The Supplier shall make available to Micro Focus on request in a timely manner (and in any event within two (2) Business Days):

6.2.1 copies of the records under clause 6.1; and

6.2.2 such other information as Micro Focus reasonably requires to demonstrate the Supplier's compliance with its obligations under data protection laws and this Variation Agreement.

6.3 The Supplier shall at no cost to Micro Focus:

6.3.1 allow for and contribute to audits, including inspections, conducted by Micro Focus or another auditor mandated by Micro Focus for the purpose of demonstrating compliance by the Supplier with its obligations under data protection laws and under this Schedule;

6.3.2 allow for and contribute to Privacy and/or Data Privacy Impact Assessments; and

6.3.3 provide (and procure) reasonable access for Micro Focus or such other auditor (where practicable, during normal business hours) to:

(a) the facilities, equipment, premises and sites on which Data and/or the records referred to in clause 6.1 are held, and to any other equipment or facilities used in the provision of the Services (in each case whether or not owned or controlled by the Supplier); and

(b) to the Supplier Personnel, provided that Micro Focus gives the Supplier reasonable prior notice of such audit and/or inspection.

6.4 If any audit or inspection reveals a material non-compliance by the Supplier with its obligations under Data Protection Laws or a breach by the Supplier of this Schedule, the Supplier shall pay the reasonable costs of the Micro Focus or its mandated auditors, of the audit or inspection.

6.5 The Supplier shall provide regular status updates, including action taken, and promptly resolve, at its own cost and expense, all data protection and security issues discovered by Micro Focus and reported to the Supplier that reveal a breach or potential breach by the Supplier of its obligations under any of this Schedule.

6.6 If the Supplier is in breach of its obligations under any of this Schedule, Micro Focus may suspend the transfer of Data to the Supplier or suspend Services, access to data, systems and network resources until the breach is remedied.

## **7. Breach Notification**

7.1 In respect of any Data Breach, the Supplier shall:

7.1.1 notify Micro Focus of the Data Breach without undue delay; and

7.1.2 provide Micro Focus without undue delay (wherever possible, no later than 24 hours after becoming aware of the Data Breach) with such details as Micro Focus reasonably requires regarding:

(a) the nature of the Data Breach, including the categories and approximate numbers of Data Subjects and Data records concerned;

(b) any investigations into such Data Breach;

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

(d) any measures taken, or that the Supplier recommends, to address the Data Breach, including to mitigate its possible adverse effects, provided that, (without prejudice to the above obligations) if the Supplier cannot provide all these details within such timeframes, it shall (before the end of this timeframe) provide Micro Focus with reasons for the delay and when it expects to be able to provide the relevant details (which may be phased), and give Micro Focus regular updates on these matters.

## **8. Deletion or Return of Data and Copies**

8.1 The Supplier shall without delay, at Micro Focus' written request, either securely delete or securely return all the Data to Micro Focus in such form as Micro Focus reasonably requests after the earlier of:

8.1.1 the end of the provision of the relevant Services related to processing; or

8.1.2 once processing by the Supplier of any Data is no longer required for the purpose of the Supplier's performance of its relevant obligations under this Agreement, and securely delete existing copies on all devices or technically feasible, use a remote wipe capability (unless storage of any data is required by applicable law and, if so, the Supplier shall inform Micro Focus of any such requirement), and provide a certificate of destruction.

## **9. Responsibilities**

9.1 Nothing in this Agreement shall relieve the Supplier of its own direct responsibilities and liabilities under applicable data protection laws including its obligations to:

9.1.1 co-operating with Data Protection Supervisory Authorities and/or Privacy Regulators;

9.1.2 employing a Data Protection Officer (if required to do so); and

9.1.3 if required to do so, appoint (in writing) a representative in compliance with applicable data protection laws.

## Supplier Contract Exit Plan

The Supplier Contract Exit Plan, as a minimum, must contain the following information (at no cost and expense to Micro Focus):

1. provisions for the identification of and a timetable for the secure transfer of Micro Focus data and information to include any documents, reasonably necessary to accomplish the transfer objectives;
2. a migration plan for how the Supplier will securely transfer data of Micro Focus back to Micro Focus or to the Successor Supplier in the format required by Micro Focus;
3. provisions for the identification of the Supplier employees, key personnel and other resources that will be used and available to provide termination services and further assistance after the termination;
4. provision for the identification of the exit data and information, and the transfer to Micro Focus of:
  - a. the exit data and information not less than thirty (30) days prior to the termination of this Agreement or any Statement of Works (SOW) (or, where termination of this Agreement is on less than thirty (30) days' notice as soon as reasonably practicable after receipt of the notice of termination); and
  - b. updated version of the exit plan as at termination and at such other times as the exit plan shall specify;
5. timetable setting out the processes for the phased transfer of the services and/or supply of goods during the termination period from the Supplier to Micro Focus or Successor Supplier, including:
  - a. a detailed description of the activities to be undertaken by the Supplier, Micro Focus and any Successor Supplier, in order to affect the orderly and secure transfer of provision of the services and/or supply of goods from the Supplier to Micro Focus or any Successor Supplier;
  - b. the management structure to be employed during the transfer and cessation of the services and/or the supply of goods;
6. provision for the performance by the Supplier of the exit obligations agreed;
7. appropriate measures to minimise disruption to the supply of services and/or goods until the date of termination of this Agreement;
8. appropriate measures to minimise the costs payable to third parties by Micro Focus, as a result of termination;
9. a requirement on the Supplier, if so required by Micro Focus, to co-operate with Micro Focus in good faith and provide reasonable assistance to facilitate Micro Focus (and/or a Successor Supplier) to obtain suitable licences and/or permissions from the Supplier's providers to enable Micro Focus (and/or Successor Supplier) continued access to, and use of, IPRs required for the continued provision of services;
10. details of any exclusive third-party contracts and exclusive assets and a plan for dealing with these;
11. a list of all data and information, documentation or assistance required in connection with the implementation of the provisions of the exit plan, and where possible identification of who is to provide such data, information and documentation, or assistance and when it is to be provided;
12. an analysis of all risks and potential issues affecting the Supplier, Micro Focus and/or Successor Supplier in relation to the implementation of the termination of services;
13. an inventory of the data, information and documentation and media stored off-site;
14. provision for the orderly hand-off of ongoing projects as required by Micro Focus, including the status of current and pending projects;
15. provision for the preparation for and conduct of migration testing;
16. details of all training and other procedures that will be required in order to affect an effective knowledge transfer from the Supplier to Micro Focus and/or Successor Supplier;
17. an analysis of the impact of the transfer of the terminated services on any services that will remain subject to this Agreement;
18. post-transfer responsibilities the Supplier will perform as part of the exit plan which, at a minimum, shall include (at no cost and expense to Micro Focus):
  - a. providing reasonable assistance as requested by Micro Focus to transfer services back to Micro Focus and/or the Successor Supplier;

- b. returning to Micro Focus any remaining property and/or data of Micro Focus in the Supplier's possession, including remaining documents, data and other information and material. Alternatively, as required by Micro Focus, the Supplier shall delete and/or destroy such property and/or data;
- c. certify that all Micro Focus property, data, information and documents have been removed from the Supplier's systems, premises and control and returned or destroyed as instructed by Micro Focus.
- d. If requested by Micro Focus and upon advance notification, Micro Focus to conduct audit post exit if there is a strong need to perform in the event being requested by data subjects or compliance agency.

## ANNEX 2 – STANDARD CONTRACTUAL CLAUSES

The following Standard Contractual Clauses shall apply to the transfer of Personal Data from the European Union to processors established in third countries (controller to processor / processor to processor transfers).

### 1. DEFINITIONS

For the purposes of these Standard Contractual Clauses:

- a) 'Personal Data', 'Special Categories of Data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of Personal Data and on the free movement of such data;
- b) 'the data exporter' means the controller who transfers the Personal Data;
- c) 'the data importer' means the processor who agrees to receive from the data exporter Personal Data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer Personal Data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of Personal Data applicable to a data controller in the Member State in which the data exporter is established;
- f) 'technical and organisational security measures' means those measures aimed at protecting Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

### 2. DETAILS OF THE TRANSFER

The details of the transfer and in particular the special categories of Personal Data where applicable are specified in the attached Appendix 1 which forms an integral part of the Clauses.

### 3. THIRD-PARTY BENEFICIARY CLAUSE

- 3.1 The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6.1 and 6.2, Clause 7, Clause 8.2, and Clauses 9 to 12 as third-party beneficiary.
- 3.2 The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8.2, and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
- 3.3 The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8.2, and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
- 3.4 The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

### 4. OBLIGATIONS OF THE DATA EXPORTER

The data exporter agrees and warrants:

- a) that the processing, including the transfer itself, of the Personal Data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- b) that it has instructed and throughout the duration of the Personal Data processing services will instruct the data importer to process the Personal Data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures;
- d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- e) that it will ensure compliance with the security measures;



- f) that, if the transfer involves Special Categories of Data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8.3 to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- h) to make available to the data subjects upon request a copy of the Clauses, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the Personal Data and the rights of data subject as the data importer under the Clauses; and
- j) that it will ensure compliance with Clause 4(a) to (i).

## 5. OBLIGATIONS OF THE DATA IMPORTER

The data importer agrees and warrants:

- a) to process the Personal Data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- c) that it has implemented adequate technical and organisational security measures before processing the Personal Data transferred;
- d) that it will promptly notify the data exporter about:
  - (i) any legally binding request for disclosure of the Personal Data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
  - (ii) any accidental or unauthorised access, and
  - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the Personal Data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information;
- h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;
- i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;
- j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

## 6. LIABILITY

6.1 The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive reasonable compensation from the data exporter for the damage suffered.

6.2 If a data subject is not able to bring a claim for compensation in accordance with paragraph 6.1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the importer shall be limited to its own processing operations under the Clauses. The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

6.3 If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 6.1 and 6.2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to

its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

## 7. MEDIATION AND JURISDICTION

- 7.1 The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
- to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
  - to refer the dispute to the courts in the Member State in which the data exporter is established.
- 7.2 The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

## 8. COOPERATION WITH SUPERVISORY AUTHORITIES

- 8.1 The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
- 8.2 The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
- 8.3 The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 8.2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

## 9. GOVERNING LAW

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

## 10. VARIATION OF THE CONTRACT

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clauses.

## 11. SUB-PROCESSING

- 11.1 The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, 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 the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.
- 11.2 The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in Clause 6.1 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
- 11.3 The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 11.1 shall be governed by the law of the Member State in which the data exporter is established.
- 11.4 The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

## 12. OBLIGATION AFTER THE TERMINATION OF PERSONAL DATA PROCESSING SERVICES

- 12.1 The parties agree that on the termination of the provision of data processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the Personal Data transferred and the copies thereof to the data exporter or shall destroy all the Personal Data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the Personal Data transferred. In that case, the data importer warrants that it will guarantee the security and confidentiality of the Personal Data transferred and will not actively process the Personal Data transferred anymore.
- 12.2 The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 12.1 and Clause 5(f).

**Appendix 1**  
**To the Standard Contractual Clauses**

This Appendix forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

**Data exporter**

The data exporter is (please specify briefly your activities relevant to the transfer):

...  
...  
...

**Data importer**

The data importer is (please specify briefly activities relevant to the transfer):

...  
...  
...

**Data subjects**

The personal data transferred concern the following categories of data subjects (please specify):

...  
...  
...

**Categories of data**

The personal data transferred concern the following categories of data (please specify):

...  
...  
...

**Special categories of data (if appropriate)**

The personal data transferred concern the following special categories of data (please specify):

...  
...

**Processing operations**

The personal data transferred will be subject to the following basic processing activities (please specify):

...  
...

DATA EXPORTER

Name:

Authorised Signature

DATA IMPORTER

Name:

Authorised Signature

**Appendix 2**  
**To the Standard Contractual Clauses**

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

...  
...  
...  
...

**[REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]**

## APPENDIX 1

### To Supplier Data Privacy and Protection Variation Agreement REQUIREMENTS OF SECTION 11 – GERMAN FEDERAL DATA PROTECTION ACT (“FDPA”)

1. In order to fully comply with mandatory provisions of Section 11 FDPA regarding the commissioning of the data importer as a processor under the national laws applicable to the data exporter, the parties agree on the following amendments to the Standard Contractual Clauses:
  - (a) Data importer will rectify, delete, return and/or block personal data if so instructed by data exporter.
  - (b) Data importer shall control, in an appropriate way, compliance with its data protection obligations and provide related reports to data exporter.
  - (c) Data exporter shall have the right to control compliance of data importer with its data protection obligations (especially with the administrative, physical, technical and organizational measures implemented or to be implemented) by adequate and reasonable means (e.g., by requesting information, assessments or audit reports regarding the data importer's data processing systems), it being understood that such measures may only relate to information and data processing systems that are relevant to the services. Data importer shall support and extend cooperation to data exporter in carrying out such controls to the reasonably necessary extent without any charge or cost to the data exporter. Upon request the data importer shall prove to the data exporter that the administrative, physical, technical and organizational measures agreed in Annex 1 have been implemented.
  - (d) Data importer shall notify data exporter, without undue delay, if it holds that an instruction violates applicable law. Upon such notification, data importer shall have the right to refrain from or discontinue (as the case may be) carrying out the instruction until data exporter has confirmed or changed the instruction. Data importer will notify the data exporter about all requests by data subjects to access, rectify, delete or block personal data, about all complaints by data subjects and objections of competent data protection authorities and all other risks and violations.
  - (e). Data importer shall ensure that any of its or any of its subcontractors' personnel entrusted with processing personal data under these Clauses (i) have undertaken to comply with the principle of data secrecy (i.e. to not collect, process or use personal data without authorization by the data exporter), and (ii) have been duly instructed on the protective regulations of the applicable data protection laws.
  - (f) Data importer shall notify to data exporter the contact details of the data importer's data protection official (if one was appointed or a named individual that is responsible and available to deal with data protection issues as and when they arise).
  - (g) Data exporter shall have the right to instruct data importer, both on a general and a case-specific basis, regarding the "if" and "how" of the collection, processing and use of personal data in connection with the services. Instructions may also relate to the rectifying, deletion and/or blocking of data. Instructions shall be given as a rule, except where the urgency or other circumstances require that an instruction be given in a different form (e.g., orally, per e-mail etc.).
  - (h) Unless otherwise instructed by the data exporter the data importer may return all data being subject of this agreement to the data exporter at the end of the contract and refrain from any further processing and use of the data, if possible for the data importer without violating its own legal duties.
  - (i) The term of these Clauses corresponds to the term of the Commercial Agreement entered into by data exporter and data importer. These Clauses shall automatically terminate upon any termination or expiration of the Commercial Agreement.
2. If and to the extent necessary to comply with mandatory provisions regarding the commissioning of the data importer as a processor under the national laws applicable to the data exporter, data exporter may propose any necessary amendments to these provisions. Such amendments are deemed accepted by the data importer if it does not reject the changes within four weeks after having received a notification of the amendments. The data importer shall be informed about this consequence in the notification. If disputed, the necessity of an amendment shall be deemed proven if the data exporter presents a respective order (which may be informal) by a competent regulator. The data exporter is not obliged to demand that the regulator issues a formal order, or to challenge an informal order.
3. In the event of inconsistencies between this appendix and the Standard Contractual Clauses the provisions of the Standard Contractual Clauses shall prevail. Provisions of this Appendix shall however remain valid to the extent that they do not contradict but merely amend the provisions of the Standard Contractual Clauses.
4. Should any provision or condition of this Appendix be held or declared invalid, unlawful or unenforceable by a competent authority or court, then the remainder of this Appendix shall remain valid. Such an invalidity, unlawfulness or unenforceability shall have no effect on the other provisions and conditions of this Appendix. The provision or condition affected shall be either (i) amended to an extent that ensures its validity, lawfulness and enforceability, while preserving the parties' intentions, or (ii) construed in a manner as if the invalid, unlawful or unenforceable part had never been contained therein.