

Data Processing Agreement

(hereinafter referred to as "**Data Processing Agreement**")

by and between

1. Flexera Software Limited, Level 3, 401 Faraday Street Birchwood Park, Birchwood Warrington, Cheshire, WA3 6GA, United Kingdom.

- hereinafter referred to as "**Flexera**" -

and

- 2.

- hereinafter referred to as "**Customer**" -

- Flexera and Customer hereinafter referred to as "**Parties**" and each as "**Party**" -

**PREAMBLE**

Flexera is a software manufacturing company which offers license management software as a service ("**SaaS**") and/or maintenance services, hereinafter altogether called ("**Services**") in accordance with the Software License and Services Agreement including any related service agreements entered into between the Parties ("**Master Agreement**"). In the course of providing the Services, Flexera will process personal data within the meaning of Art. 4 no 1 and 2 of the General Data Protection Regulation (Regulation 2016/679 – "**GDPR**") of Customer and/or Customer's affiliates including the data of their customers located in the European Union or European Economic Area ("**Customer Personal Data**").

This Data Processing Agreement regulates the data protection obligations of the Parties when processing Customer Personal Data under the Master Agreement and will reasonably ensure that such processing will only be rendered on behalf of and under the Instructions of Customer and in accordance with Art. 28 and 29 GDPR.

**DEFINITIONS**

- "**Affiliate**" means a Customer affiliate who is a beneficiary under the Master Agreement or any purchase order based thereon;
- "**Applicable Law**" means all laws, rules and regulations applicable to either party's performance under this Data Processing Agreement, including but not limited to those applicable to the processing of personal data. This means in particular the GDPR and all national laws validly amending the applicable rules for the processing of personal data.
- "**European State**" means any country in the European Economic Area (consisting of the member states of the European Union together with Iceland, Norway and Liechtenstein) as well as UK and Switzerland;

- **"Instruction"** means any documented instruction, submitted by Customer to Flexera, directing Flexera to perform a specific action with regard to personal data, including but not limited to the rectification, erasure or restriction of processing of personal data. Instructions shall initially be specified in the Master Agreement, in Sec. 2 and Exhibit A and may, from time to time thereafter, be amended, supplemented or replaced by Customer by separate written or text form instructions, provided that such instructions still fall within the scope of the Services. Instructions issued for the purpose of complying with statutory claims under the GDPR such as rectification, erasure, restriction or portability of personal data fall within the scope of the Services.
- Terms used but not defined in this Data Processing Agreement, including but not limited to "personal data", "personal data breach", "processing", "controller", "processor" and "data subject", shall have the same meaning as set forth in Art. 4 GDPR.

## **1. AMENDMENT OF MASTER AGREEMENT**

- 1.1 This Data Processing Agreement amends the Master Agreement with respect to any processing of Customer Personal Data provided by Customer or Affiliate if Customer or, respectively, the Affiliate (i) is located in a European State or (ii) processes personal data of data subjects who are located in a European State.
- 1.2 Customer, respectively, its Affiliate, is the controller of personal data and Flexera is the processor of such data, except when Customer or Affiliate acts as a processor of personal data, in which case Flexera is a subprocessor.

## **2. SUBJECT MATTER, DURATION, NATURE AND PURPOSE, AND SPECIFICATION OF PROCESSING OPERATIONS**

- 2.1 The subject matter, duration, nature and purpose of the processing are described in this Sec. 2 and the Master Agreement. Unless provided for otherwise in the Master Agreement, the processing will generally be limited to (i) the storage/processing of certain limited Customer Personal Data on a server and incidental access to such data when providing the SaaS services pursuant to the Master Agreement, and/or (ii) when rendering maintenance services for on-premise solutions. However, when rendering compliance intelligence services, Customer Personal Data may be accessed by the data success and support team for the purpose of providing the services as agreed in the Master Agreement. All of the aforementioned described processing also includes the use of data for testing for purposes of improving the Customer's services. When providing on-premise maintenance, there shall be no access to or processing of Customer Personal Data but incidental access to such data stored on Customer's premises cannot be excluded. When Flexera cooperates with partners having an own direct customer relationship with their customers and where those partners need access to the data of their customers (all of which is part of the Customer Personal Data) for purposes of assisting with services, Flexera grants such partners access to such Customer Personal Data to the extent needed for such purposes.
- 2.2 The following types of personal data and categories of data subjects may be affected by the processing:

- Categories of data subjects: Employees, contractors, agents etc. of Customer or Affiliate and the employees of Customer's or Affiliate's contractors, agents, etc. as well as the Customer's or Affiliate's customers' employees, and the employees of their contractors, agents, etc.
- Types of personal data: Names, usernames, user IDs, business/personal addresses, phone numbers, departments, email addresses, and IP addresses, computer or device names, Ethernet MAC Addresses, host names, calculated users, account names, serial numbers, virtual Machine UUIDs, hardware dongleIDs, time zones, active directory names, FQDNs, Wi-Fi SSIDs, geolocation data.
- Special Categories of personal data: None.

When rendering maintenance services, the following types of personal data and categories of data subjects may be affected:

- Any kind of personal data which is stored on Customer's premises and which relates to any kind of data subjects.

2.3 The duration of the processing shall correspond to the duration of this Data Processing Agreement as set forth in Sec. 8.

### **3. FLEXERA'S OBLIGATIONS**

3.1 Flexera shall in the course of providing Services, including with regard to transfers of personal data to a third country, process Customer Personal Data only on behalf of and under the documented Instructions of Customer unless required to do so otherwise by the law of the European Union or European State; in such a case, Flexera shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. Should Flexera be bound to process Customer Personal Data otherwise in order to comply with the law of the United Kingdom, Flexera shall inform the Customer or the Affiliate of such legal obligation and grant to Customer the ability to terminate this Data Processing Agreement with immediate effect in the case that such processing would conflict with GDPR requirements. Flexera shall remain entitled to claim its agreed remuneration until the term end.

3.2 Flexera shall take steps reasonably necessary to ensure that any natural person acting under its authority who has access to personal data does not process such data except on Instructions from Customer, unless otherwise required to do so by the law of the European Union or a European State. The provisions contained in Sec. 3.1, 2<sup>nd</sup> and 3<sup>rd</sup> sentence shall apply accordingly.

3.3 Flexera ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and that the obligation will remain after termination of this Data Processing Agreement.

3.4 Technical and Organizational Data Security Measures

3.4.1 The appropriate technical and organizational data security measures implemented at the date of the signing of this Data Processing Agreement are specified in Exhibit A. The measures specified in Exhibit A are subject to technical advancements and development.

- 3.4.2 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Flexera shall implement and maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk, as required by Art. 32 GDPR. As appropriate, this may include
- the pseudonymization and encryption of personal data;
  - the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; and
  - the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
- 3.4.3 When assessing the appropriate level of security, account shall be taken in particular of the nature, scope, context and purpose of the processing as well as the risks that are presented by the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.
- 3.4.4 If Flexera significantly modifies measures specified in Exhibit A, such modifications have to meet the obligations pursuant to Sec. 3.4.2 and 3.4.3. Flexera shall make available to Customer a description of such measures which enables Customer to assess compliance with Art. 32 GDPR. By notifying, Flexera grants to Customer the opportunity to object to such modifications within four (4) weeks. Customer shall only be entitled to object to any modification in the case that the modification does not meet the requirements pursuant to Sec. 3.4.2 and 3.4.3. If Customer does not object to the modification within the objection period, consent regarding the modifications shall be assumed. In case of an objection, Flexera may suspend the portion of the Service which is affected by the objection of Customer. Customer shall not be entitled to a pro-rata refund of remuneration for the Services, unless Customer can prove that the obligations pursuant to Sec. 3.4.2 and 3.4.3 have not been met.
- 3.4.5 Flexera shall implement a data protection management procedure according to Art. 32 para 1 lit. d) GDPR, for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures to reasonably ensure the security of the processing. Flexera will further, by way of regular self-audits, reasonably ensure that the processing of Customer Personal Data conforms with the provisions as agreed with Customer or to Customer's Instructions.
- 3.5 Flexera shall, while taking into account the nature of the processing, assist Customer through appropriate technical and organizational measures, with the fulfilment of Customer's obligations to respond to requests for exercising rights of data subjects in accordance with Applicable Law, in particular Art. 15 through 18 and 21 GDPR.
- 3.6 Taking into account the nature of the processing and the information available to Flexera, Flexera shall assist Customer with ensuring compliance with the obligations pursuant to Art. 33 through 36 GDPR (Data Security Breach Notification, Data Protection Impact Assessment, Consultation

with Data Protection Supervisory Authorities), in particular by providing information concerning Customer Personal Data.

### 3.7 Documentation and Audit Rights

3.7.1 Upon request and subject to a non-disclosure agreement, Flexera shall provide to Customer a comprehensive documentation of the technical and organizational data security measures in accordance with industry standards. The effectiveness of Flexera's technical and organizational security measures will be audited by an independent third-party on an annual basis, in an SSAE16 SOC 2 Type II audit or equivalent. In addition, Flexera may, in its discretion provide data protection compliance certifications issued by a commonly accepted certification issuer which has been audited by a data security expert, by a publicly certified auditing company or by another customer of Flexera.

3.7.2 If Customer has justifiable reason to believe that Flexera is not complying with the terms and conditions under this Data Processing Agreement, in particular with the obligation to implement and maintain the agreed technical and organizational data security measures, and only once per year (unless there are specific indications that require a more frequent inspection), Customer is, subject to a non-disclosure agreement, entitled to audit Flexera. This audit right can be exercised by (i) requesting additional information, (ii) accessing the databases which process Customer Personal Data or (iii) by inspecting Flexera's working premises whereby in each case no access to personal data of other customers or Flexera's confidential information will be granted. Alternatively, Customer may also engage third party auditors to perform such tasks on its behalf in accordance with Sec. 3.7.4. The costs associated with such audits and/or for providing additional information shall be borne by Customer unless such audit reveals Flexera's material breach with this Data Processing Agreement.

3.7.3 If Customer intends to conduct an audit at Flexera's working premises, Customer shall give reasonable notice to Flexera and agree with Flexera on the time and duration of the audit. In the case of a special legitimate interest, such audit can also be conducted without prior notice. Inspections shall be made during regular business hours and in such a way that business operations are not disturbed. At least one employee of Flexera may accompany the auditors at any time. Flexera may memorialize the results of the audit which shall be confirmed by Customer.

3.7.4 Customer may not appoint a third party as auditor who (i) Flexera reasonably considers to be in a competitive relationship to Flexera or (ii) is not sufficiently qualified to conduct such an audit, or (iii) is not independent. Any such third-party auditor shall only be engaged if the auditor is bound by a non-disclosure agreement in favor of Flexera prior to conducting any audit or is bound by statutory confidentiality obligations.

### 3.8 Notification Duties

3.8.1 Flexera shall inform Customer without undue delay in text form (e.g., letter, fax or email "**Text Form**") of the following events:

- Requests from third parties including such from a data protection supervisory authority and data subjects regarding Customer Personal Data; in which case it is permitted to inform the third party of the name of Customer and the fact that it has forwarded the request to Customer.
- Threats to Customer Personal Data in possession of Flexera by garnishment, confiscation, insolvency and settlement proceedings or other incidents or measures by third parties. In such case, Flexera shall immediately inform the respective responsible person/entity that Customer holds the sovereignty and ownership of the personal data.

3.8.2 For the purpose of enabling Customer to comply with its own data breach notification obligations pursuant to Art. 33 para 1 and Art. 34 para 1 GDPR, Flexera shall notify Customer without undue delay after becoming aware of a personal data breach. Such notice will, if possible, include the following information:

- a description of the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;
- a description of the measures taken or proposed to be taken by Flexera and/or Customer to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects; and
- any further information which is available and known to Flexera and (i) that is necessary for Customer to comply with Customer's notification obligations and (ii) which Customer does not otherwise have access to.

3.8.3 Flexera shall inform Customer immediately if, from its point of view, an Instruction of Customer may lead to a violation of the GDPR or other data protection law of the European Union or a European State. Until Customer either confirms or alternates the Instruction, Flexera may refuse to comply with the Instruction issued.

### 3.9 Rectification, Erasure, Restriction

3.9.1 If legally required and Customer is unable to perform the applicable task itself, or if provided so in the services description contained in the Master Agreement, Flexera shall rectify, erase, restrict or transmit Customer Personal Data upon Customer's request as soon as possible but at the latest within 30 days upon notice. Any erasure of Customer Personal Data pursuant to this Sec. 3.9 shall be executed in such a manner that restoring or recovering such data is rendered reasonably impossible.

3.9.2 At Customer's request, Flexera shall conduct a data protection-compliant destruction of data media and other material provided by Customer. Alternatively, at the request of Customer, Flexera shall provide the data carriers and other material to Customer or store it on Customer's behalf.

- 3.9.3 Unless the law of the European Union or a European State requires a continued retention of the personal data, Flexera shall, upon completion of the Services in consultation with Customer, either delete or return all Customer Personal Data in its possession to Customer. The provision contained in Sec. 3.1, 2<sup>nd</sup> and 3<sup>rd</sup> sentence shall apply accordingly.
- 3.9.4 If a data subject addresses Flexera with claims for access, rectification, erasure, restriction, objection or data portability, Flexera shall refer the data subject to Customer.
- 3.10 Flexera will inform Customer of the name and the official contact details of its data protection officer if Flexera is, by Applicable Law, required to appoint a data protection officer. If Flexera is not required to appoint a data protection officer, Flexera shall – in its own discretion – name a person responsible for dealing with questions relating to applicable data protection law and data security in the context of performing this Data Processing Agreement.
- 3.11 In the case claims based on Art. 82 GDPR are raised against Customer, Flexera shall reasonably support Customer with its defense to the extent the claim arises in connection with the processing of personal data by Flexera in connection with performing the Services to Customer.
- 3.12 Flexera will make available to Customer all information necessary to demonstrate compliance with the obligations laid down in this Data Processing Agreement and Art. 28 GDPR.
- 3.13 Flexera will on request make available to a supervisory authority records of its processing activities based on Art. 30 GDPR.
- 3.14 Unless otherwise described in Sec. 5, any data processing shall take place in the United Kingdom or in countries of the European Union.

#### **4. CUSTOMER'S OBLIGATIONS**

- 4.1 Customer shall provide all Instructions pursuant to this Data Processing Agreement to Flexera in Text Form or verbally. Verbal Instructions shall be confirmed immediately in Text Form thereafter.
- 4.2 Customer shall notify Flexera in Text Form of the names of the persons who are entitled to issue Instructions to Flexera. Any consequential costs incurred resulting from Customer's failure to comply with the preceding sentence shall be borne by Customer. In any event, the managing directors and personnel/human resource management of Customer are entitled to issue Instructions.
- 4.3 Customer shall inform Flexera immediately if processing by Flexera might lead to a violation of data protection regulations.
- 4.4 In the case claims based on Art. 82 GDPR are raised against Flexera, Customer shall reasonably support Flexera with its defense to the extent the claim arises in connection with the processing of personal data by Flexera in connection with performing the Services to Customer or Affiliate.

4.5 Customer shall name a person responsible for dealing with questions relating to applicable data protection law and data security in the context of performing this Data Processing Agreement.

## 5. SUBPROCESSING

5.1 Flexera may engage third parties to perform the agreed processing activities under this Data Processing Agreement ("**Subcontractor**") subject to the requirements pursuant to this Sec. 5.

5.2 Any Subcontractor is obliged, before initiating the processing, to commit itself in writing for the benefit of Customer and its Affiliates to comply with the same data protection obligations as the ones under this Data Processing Agreement or legal act within the meaning of Art. 28 para 3, 4 and 6 GDPR unless explicitly agreed otherwise. The agreement with the Subcontractor must provide at least the level of data protection required by this Data Processing Agreement. Where the Subcontractor fails to fulfil its data protection obligations, Flexera shall remain fully liable to Customer for the performance of the Subcontractor's obligations.

5.3 Any Subcontractor must in particular agree to comply with the agreed technical and organizational security measures in accordance with Sec. 3.4.2 and 3.4.3 herein and provide Flexera with a list of the implemented technical and organizational measures, which upon request by Customer will also be made available to Customer. Subcontractor's measures may differ from the ones agreed between Customer and Flexera but shall not fall below the level of data security as provided by the measures of Flexera.

5.4 In the case a Subcontractor is located outside the European Union/European Economic Area and not in a country/territory which, pursuant to Art. 45 GDPR, provides for an adequate level of data protection, Flexera shall, conclude a data processing agreement based on the EU Standard Contractual Clauses for Processors (notified under document C (2010)593) or any other standard protection clauses for processors as permitted under Art. 46 para 2 (c) GDPR with that Subcontractor. Flexera shall also be entitled to conclude Standard Contractual Clauses or any other standard protection clauses in the name and for the benefit of Customer. Customer herewith authorizes Flexera to conclude such agreement in its own name.

5.5 Where a Subcontractor refuses to be bound by the same data protection obligations as the ones under this Data Processing Agreement, Customer may consent thereto, whereby such consent shall not be unreasonably withheld.

5.6 Flexera will inform Customer in Text Form of any intended engagement of a Subcontractor. Alternatively, Flexera may provide a website or provide another notice that lists all Subcontractors to access personal data of its Customer as well as the limited or ancillary services they provide. At least two (2) weeks before authorizing any new Subcontractor to access personal data, Flexera will notify Customer thereof and, if applicable, update its website. By notifying, Flexera grants to Customer the opportunity to object to such change within two (2) weeks. If Customer does not object to the engagement within the objection period, consent regarding the engagement shall be assumed. Upon Customer's request, Flexera will provide all information necessary to demonstrate that the Subcontractor will meet all requirements pursuant to Sec. 5.3. In the case Customer objects to the subprocessing, Flexera can choose to either not engage the Subcontractor or to terminate the Master Agreement with two (2) months prior written notice. Until the termination of the Master Agreement, Flexera may suspend the portion of the Services which is affected by the objection of



Customer. Customer shall not be entitled to a pro-rata refund of the remuneration for the Services, unless the objection is based on justified reasons of non-compliance with applicable data protection law.

5.7 Customer herewith agrees also on behalf of its Affiliates to the following Subcontractors:

**For all Spider and Columbus Products and Services:**

For Professional Services:

- Flexera Software GmbH, Paul-Dessau-Straße 822761 Hamburg, Germany.

For all kinds of Services:

- Spider Lifecycle Managementsysteme GmbH, Paul-Dessau-Straße 8, 22761 Hamburg, Germany;
- Flexera Software LLC, 300 Park Blvd, Suite 500, Itasca, IL 60143, USA. For any transfer we rely on an Intra-Group-Data-Processing-Agreement which includes also the Standard Contractual Clauses for Processors;
- Flexera Software Limited, Level 3, 401 Faraday Street Birchwood Park, Birchwood Warrington, Cheshire, WA3 6GA, United Kingdom;
- Brainware Solutions AG, Sumpfstrasse 15, CH-6312 Steinhausen, Switzerland.

**For all other Flexera Products and Services:**

For Software Monetization Services:

- Akamai International B.V. Prins Bernhardplein 200, JB Amsterdam 1097, The Netherlands, provides our content delivery network services.
- Akamai Technologies Inc. 150 Broadway, Cambridge, MA 02142, USA, provides our content delivery network services.
- Snowflake Inc., Suite 3A, 106 East Babcock Street, Bozeman, Montana 59715, USA, provides data warehousing services.

For Software Licensing Optimization and Data Platform Services:

- GoodData Corporation, 660 3rd Street Suite 101, San Francisco, CA 94107, USA, conducts analytic services as well as data platform services. For any transfer we rely on data processing agreements containing the Standard Contractual Clauses for Processors.

For Software Vulnerability Management:

- Secunia ApS, Mikado House, Rued Langgaards Vej 8, 4th floor, Copenhagen, S DK-2300, Denmark, is mainly in charge of implementing IT security solutions and rendering support and maintenance services for Flexera.

For Cloud Delivery Services:

- RightScale, Inc. 402 E. Gutierrez Street, Santa Barbara, CA 93101, USA. For any transfer we rely on an Intra-Group-Data-Processing-Agreement including also the Standard Contractual Clauses for Processors.

For SaaS Services:

- Intercom, Inc. 55 2nd Street, 4th Fl., San Francisco, CA 94105, USA. For any transfer we rely on data processing agreements containing the Standard Contractual Clauses for Processors.

For Compliance and Usage Intelligence Services:

- Revulytics Inc., 130 Turner Street, Building 2, Suite 212, Waltham, Massachusetts 02453. For any transfer we rely on an Intra-Group-Data-Processing-Agreement which includes the Standard Contractual Clauses for Processors.
- Infnit-O Global, Limited, 24/F Pacific Star Building, Sen. Gil Puyat corner Makati Avenue, Makati, 1200 Metro Manila. For any transfer we rely on data processing agreements containing the Standard Contractual Clauses for Processors.

For Hosting Services:

- Amazon Web Services, Inc., 410 Terry Avenue North, Seattle WA 98109, USA. For any transfer we rely on data processing agreements containing the Standard Contractual Clauses for Processors.

For Professional Services:

- Flexera Software GmbH, Paul-Dessau-Straße, 822761 Hamburg, Germany.

For all kinds of Services:

- Flexera Software LLC, 300 Park Blvd, Suite 500, Itasca, IL 60143, USA. For any transfer we rely on an Intra-Group-Data-Processing-Agreement which includes the Standard Contractual Clauses for Processors.

5.8 Upon Customer's request, Flexera shall provide Customer with information on relevant data protection obligations of Subcontractor, which shall include, but not be limited to, granting necessary access to the relevant contractual documents.

5.9 Flexera shall audit its Subcontractor on a regular basis and will, upon Customer's request, confirm their compliance with data protection law and the obligations set upon the Subcontractor according to the data processing agreement concluded with them. Only in the case of justified reasons, Customer shall issue Instructions to Flexera to conduct further audits that Flexera will conduct to the extent permissible.

## 6. LIABILITY

6.1 Customer and Flexera shall be each liable for damages of affected data subjects according to Art. 82 GDPR (external liability).

- 6.2 Either Party shall be entitled to claim back from the other Party, Flexera or Customer, that part of the compensation, corresponding to the other Party's part of responsibility for the damage (internal liability).
- 6.3 As regards the internal liability and without any effect as regards the external liability towards data subjects, the Parties agree that notwithstanding anything contained hereunder, when providing the Services, Flexera's liability for breach of any terms and conditions under this Data Processing Agreement shall be subject to the liability limitations agreed in the Master Agreement.
- 6.4 No Affiliate shall become beneficiary of this Data Processing Agreement without being bound by this Data Processing Agreement and without accepting this liability limitation.
- 6.5 Customer will indemnify Flexera against any losses that exceed the liability limitations in the Master Agreement suffered by Flexera in connection with any claims of Affiliates or data subjects who claim rights based on alleged violation of the GDPR or this Data Processing Agreement.

## **7. COSTS FOR ADDITIONAL SERVICES**

If Customer's Instructions lead to a change from or increase of the agreed Services or in the case of Flexera's compliance with its obligations pursuant to Sec. 3.6, 3.9 or 3.11 to assist Customer with Customer's own statutory obligations, Flexera is entitled to charge reasonable fees for such tasks which are based on the prices agreed for rendering the Services and/or notified to Customer in advance.

## **8. CONTRACT PERIOD**

The duration of this Data Processing Agreement coincides with the duration of the Master Agreement. It commences and terminates with the provision of the Services under the Master Agreement, unless otherwise stipulated in the provisions of this Data Processing Agreement.

## **9. MODIFICATIONS**

Flexera may modify or supplement this Data Processing Agreement, with notice to Customer, (i) if required to do so by a supervisory authority or other government or regulatory entity, (ii) if necessary to comply with Applicable Law, (iii) to implement standard contractual clauses laid down by the European Commission or (iv) to adhere to an approved code of conduct or certification mechanism approved or certified pursuant to Articles 40, 42 and 43 of the GDPR. Customer shall notify Flexera if it does not agree to a modification, in which case Flexera may terminate this Data Processing Agreement and the Master Agreement with two (2) weeks' prior written notice, whereby in the case of an objection not based on incompliance of the modifications with applicable data protection law, Flexera shall remain entitled to claim its agreed remuneration until the term end.

## **10. BREXIT PROVISION**

- 10.1 If the withdrawal agreement entered into between the United Kingdom and the European Union expires without the United Kingdom being recognized by the European Commission as a third country that provides for an adequate level of data protection, the Standard Contractual Clauses attached hereto as Exhibit B ("SCC") shall apply between Flexera and Customer in addition to these Terms of Data Processing. In this case, Flexera shall act as data importer and Customer as

data exporter. The other information to be provided according to Appendix 1 SCC shall be included by reference to Sec. 2.1 through 2.2 and the Master Agreement. Exhibit B of these Terms of Data Processing shall serve as Appendix 2 SCC. Sec. 6.2 to 6.5 shall apply respectively to the SCC. Where the scope of the definitions in Art. 4 GDPR go beyond of what is defined in the SCC, the broader understanding shall apply.

- 10.2 Flexera and Customer shall amend this Data Processing Agreement in the case that the amendments are necessary due to statutory data protection provisions of the United Kingdom. In the case that such necessary amendments would conflict with GDPR requirements, both Parties shall be entitled to immediately terminate the Master Agreement and this Data Processing Agreement. Flexera shall remain entitled to claim its agreed remuneration until the term end.

**11. WRITTEN FORM**

Any side agreements to this Data Processing Agreement as well as changes and amendments of this Data Processing Agreement or the Services hereunder, including this Sec. 11, shall be in writing.

**12. CHOICE OF LAW**

This Data Processing Agreement is governed by, and shall be interpreted in accordance with, the laws of the place of establishment of Customer, unless otherwise stipulated in the SCC if applicable.

**13. MISCELLANEOUS**

- 13.1 With respect to any issues arising of or in connection with the processing of personal data, this Data Processing Agreement shall prevail over all other agreements between the Parties.
- 13.2 In the event a clause under the Master Agreement has been found to violate the GDPR or any other Applicable Laws, the Parties will mutually agree on modifications to the Master Agreement to the extent necessary to ensure data privacy-law compliant processing.

Signatures:

\_\_\_\_\_

Customer

\_\_\_\_\_

Flexera

## **Exhibit A – Description of the Technical and Organizational Security Measures**

Sub-Processors will be bound to adhere to similar but not necessarily identical organizational security measures which, however, shall not fall below the level of data security as agreed herein. Any organizational security measures are subject to change of technical standards and can be adopted. If so requested, Flexera will provide Customer with a description of the then current measures.

### **1. Pseudonymization and Encryption, Art. 32 para 1 point a GDPR**

Pseudonymization contains measures that enable one to process personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that this additional information is stored separately, and is subject to appropriate technical and organizational measures. Encryption contains measures that enable one to convert clearly legible information into an illegible string by means of a cryptographic process.

- Stored data is encrypted where appropriate, including any backup copies of the data

### **2. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, Art. 32 para 1 point b GDPR**

Confidentiality and integrity is ensured by the secure processing of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage.

#### **2.1 Confidentiality**

##### **2.1.1. Physical access control**

Measures that prevent unauthorized persons from gaining access to data processing systems with which personal data are processed or used.

- Physical access control systems
- Definition of authorized persons and Management and documentation of individual authorizations
- Regulation of Visitors and external staff
- Monitoring of all facilities housing IT systems
- Logging of physical access

##### **2.1.2 System/Electronic access control**

Measures that prevent data processing systems from being used without authorization.

- User Authentication by simple authentication methods (using username/password)
- Secure transmission of credentials using networks (using TSL and SSL)
- Automatic account locking
- Guidelines for Handling of passwords
- Definition of authorized persons
- Managing means of authentication
- Access control to infrastructure that is hosted by cloud service provider

##### **2.1.3 Internal Access Control**

Measures that ensure that persons entitled to use a data processing system have access only to the data to which they have a right of access, and that personal data cannot be read, copied, modified or removed without authorization in the course of processing or use and after storage.

- Automatic and manual locking
- Access right management
- Access right management including authorization concept, implementation of access restrictions, implementation of the "need-to-know" principle, managing of individual access rights.

#### **2.1.4 Isolation/Separation Control**

Measures to ensure that data collected for different purposes can be processed (storage, amendment, deletion, transmission) separately.

- Network separation
- Segregation of responsibilities and duties
- Document procedures and applications for the separation

#### **2.1.5 Job Control**

Measures that ensure that, in the case of commissioned processing of personal data, the data are processed strictly corresponding the instructions of the principal.

- Training and confidentiality agreements for internal staff and external staff

### **2.2. Integrity**

#### **2.2.1 Data transmission control**

Measures ensure that personal data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged.

- Secure transmission between client and server and to external systems by using industry-standard encryption
- Secure network interconnections ensured by Firewalls etc.
- Logging of transmissions of data from IT system that stores or processes personal data

#### **2.2.2 Data input control**

Measures that ensure that it is possible to check and establish whether and by whom personal data have been input into data processing systems, modified or removed.

- Logging authentication and monitored logical system access
- Logging of data access including, but not limited to access, modification, entry and deletion of data
- Documentation of data entry rights and partially logging security related entries.

### **2.3 Availability and Resilience of Processing Systems and Services**

Availability includes measures that ensure that personal data is protected from accidental destruction or loss due to internal or external influences. Resilience of processing systems and services includes

measures that ensure the ability to withstand attacks or to quickly restore systems to working order after an attack.

- Tape-media based backup solution
- Implementation of transport policies
- Backup Concept
- Protection of stored backup media

**3. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, Art. 32 para 1 point c GDPR**

Organizational measures that ensure the possibility to quickly restore the system or data in the event of a physical or technical incident.

- Continuity planning (Recovery Time Objective)

**4. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing, Art. 32 para 1 point d GDPR**

Organizational measures that ensure the regular review and assessment of technical and organizational measures.

- Testing of emergency equipment
- Documentation of interfaces and personal data fields
- Internal assessments

## **Exhibit B – Standard Contractual Clauses for Processors**

### **Standard Contractual Clauses for Processors**

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Customer and/or each of the Affiliates are hereinafter referred to as the "**Data Exporter**" with respect to the personal data provided by the respective Data Exporter.

Flexera is hereinafter referred to as the "**Data Importer**".

The Data Exporter(s) and the Data Importer, each a "party" and collectively "the parties" HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the Data Exporter to the Data Importer of the personal data specified in **Appendix 1**.

#### *Clause 1*

#### **Definitions**

For the purposes of the 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 *'Subprocessor'* means any processor engaged by the Data Importer or by any other subprocessor of the Data Importer who agrees to receive from the Data Importer or from any other subprocessor 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 Organizational Security Measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.



*Clause 2*

***Details of the transfer***

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

*Clause 3*

***Third-party beneficiary clause***

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 (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
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. The data subject can enforce against the Subprocessor 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 Subprocessor shall be limited to its own processing operations under the Clauses.
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.

*Clause 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 Organizational Security Measures specified in Appendix 2 to this contract;
- (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, unauthorized 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 Subprocessor 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, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing 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 subprocessing, the processing activity is carried out in accordance with Clause 11 by a Subprocessor 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).

#### *Clause 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 the Technical and Organizational Security Measures specified in Appendix 2 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 unauthorized access, and
  - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized 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 subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the Data Exporter;
- (h) that, in the event of subprocessing, it has previously informed the Data Exporter and obtained its prior written consent;
- (i) that the processing services by the Subprocessor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the Data Exporter.

#### *Clause 6*

##### ***Liability***

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 Subprocessor, is entitled to receive compensation from the Data Exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the Data Exporter, arising out of a breach by the Data Importer or his Subprocessor 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 Data Importer may not rely on a breach by a Subprocessor of its obligations in order to avoid its own liabilities.
3. If a data subject is not able to bring a claim against the Data Exporter or the Data Importer referred to in paragraphs 1 and 2, arising out of a breach by the Subprocessor 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 Subprocessor agrees that the data subject may issue a claim against the data Subprocessor 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 Subprocessor shall be limited to its own processing operations under the Clauses.

#### *Clause 7*

##### ***Mediation and jurisdiction***

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:

- (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
  - (b) to refer the dispute to the courts in the Member State in which the Data Exporter is established.
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.

*Clause 8*

**Cooperation with supervisory authorities**

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.
2. The parties agree that the supervisory authority has the right to conduct an audit of the Data Importer, and of any Subprocessor, 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.
3. The Data Importer shall promptly inform the Data Exporter about the existence of legislation applicable to it or any Subprocessor preventing the conduct of an audit of the Data Importer, or any Subprocessor, pursuant to paragraph 2. In such a case the Data Exporter shall be entitled to take the measures foreseen in Clause 5 (b).

*Clause 9*

**Governing Law**

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

*Clause 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 Clause.

*Clause 11*

**Subprocessing**

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 Subprocessor which imposes the same obligations on the Subprocessor as are imposed on the Data Importer under the Clauses (This requirement may be satisfied by the Subprocessor co-signing the contract entered into between the Data Exporter and the Data Importer which is based on the terms and conditions of this Agreement.). Where the Subprocessor 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 Subprocessor's obligations under such agreement.

2. The prior written contract between the Data Importer and the Subprocessor 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 paragraph 1 of Clause 6 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 Subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the Data Exporter is established.
4. The Data Exporter shall keep a list of subprocessing 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.

*Clause 12*

***Obligation after the termination of personal data processing services***

1. The parties agree that on the termination of the provision of data processing services, the Data Importer and the Subprocessor 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 confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The Data Importer and the Subprocessor 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 1.

**APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES**

**Data Exporter**

*Customer as specified in the Data Processing Agreement is the Data Exporter.*

**Data Importer**

*Flexera as specified in the Data Processing Agreement is the Data Importer.*

**Data subjects, Categories of data, Special categories of data (if appropriate), Processing operations**

*This information shall be included by way of reference to Sec. 2.1 through 2.3 of the Data Processing Agreement and the Master Agreement.*

**APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES**

**Description of the Technical and Organizational Security Measures implemented by the Data Importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):**

Exhibit A of the Data Processing Agreement shall serve as this Appendix 2.