Data Processing Agreement

Flexera is a software company which offers a range of IT management products and services, further detail of which can be found within the Master Agreement entered into, or to be entered into, between Flexera and Customer. This Data Processing Agreement supplements the Master Agreement to ensure that any Personal Information subject to the Master Agreement is transferred to and processed by Flexera in accordance with the Applicable Privacy Laws.

1. Definitions

Unless otherwise defined, the following definitions shall apply:

1.1 **"Flexera"** means the Flexera entity described in the Master Agreement.

1.2 **"Customer"** means the Customer as described in the Master Agreement, which not only includes the contracting party, but may also encompass Customer affiliates to the extent they are beneficiaries under the Master Agreement. Customer shall be the sole contact point for Flexera under this Data Processing Agreement and any communication shall take place with and claims must be asserted by the Customer only.

1.3 **"Master Agreement"** means the agreement between Flexera and Customer which sets out the basis on which Flexera provides its products and/or services for the use of the Customer.

1.4 **"Applicable Privacy Laws"** means any applicable laws and regulations relating to the processing, privacy, or security of Personal Information.

1.5 **"Personal Information"** means any information relating to an identified or identifiable individual or device, or is otherwise "personal data," "personal information," "personally identifiable information" and similar terms, and such terms shall have the same meaning as defined by Applicable Privacy Laws.

1.6 **"Special Category or Criminal Offence Data"** means any data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation as well as data relating to criminal convictions and offences or related security measures.

2. Commencement and Scope

This Data Processing Agreement shall commence on the earlier of either (a) Flexera and Customer entering into a Master Agreement, or if earlier, (b) when Flexera commences processing Personal Information provided by Customer to Flexera in the context of the Master Agreement on behalf of Customer in connection with rendering the services as agreed under the Master Agreement ("**Services**"). This Data Processing Agreement shall remain in full force and effect as long as the Master Agreement (including any extension, renewal, or variation) remains effective and thereafter for as long as Flexera continues to process Personal Information on behalf of Customer.

3. Conflict and Order of Precedence

In the event of any conflict or inconsistency between the Master Agreement, the main body of this Data Processing Agreement, or the Schedules to this Data Processing Agreement, the following order of precedence shall apply:

3.1. Schedules of this Data Processing Agreement,

3.2. Main body of this Data Processing Agreement, and

3.3. Master Agreement.

4. Designation of Parties

4.1. Customer and Flexera agree that for the purposes of the Applicable Privacy Laws Customer is a Data Controller and Flexera is a Data Processor unless Customer is a Data Processor in which case Flexera shall be a Sub-Processor.

4.2. Customer and Flexera each agree that they shall always remain responsible for compliance with their respective obligations under the Applicable Privacy Laws.

5. Customer's Instructions

5.1. Customer instructs Flexera to process Personal Information to deliver the Services as set out within the Master Agreement. Customer may provide additional instructions in writing (email or other electronic means being sufficient) to Flexera regarding the processing of Personal Information to the extent technically feasible and provided that such instructions are still covered by the Services purchased or needed to comply with statutory rights from individuals.

5.2. Where Customer submits additional instructions or wishes to vary the existing instructions in respect of processing of Personal Information and Flexera believes that adopting the new instructions would adversely impact upon the delivery of the Services, or would lead to Flexera incurring additional costs, Flexera and Customer shall negotiate in good faith to reach an agreement in respect of either (a) varying the amended instructions, or (b) proportioning the associated costs of implementing the amended instructions.

5.3. Except with the express prior agreement of both parties' data protection officers (or other authorised representative) Customer shall not provide to Flexera any Special Category or Criminal Offence Data.

6. Sub-Processors

6.1. Where Flexera engages any third parties, whether affiliated companies or not, Flexera shall ensure that there is in place an agreement between Flexera and such party that ensures a level of protection and security comparable to what is agreed in this Data Processing Agreement including any Schedules if applicable.

The Sub-processors appointed by Flexera as set out in Schedule 1 at the commencement of this Data Processing Agreement are approved by Customer.

6.2. Where Flexera seeks to appoint a new sub-processor, it shall notify Customer of the same. In the absence of any objection from Customer within 28 days of notification, Customer shall be deemed to have consented to the appointment. If Customer wishes to object to the appointment of the intended sub-processor it should do so in accordance with the provisions of the Master Agreement. In the case Customer objects to the sub-processing, Flexera can choose to either not engage the sub-processor or to terminate the portion of the Master Agreement relating to the affected Services with 28 days 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 in compliance with Applicable Privacy Laws.

7. International Data Transfers

7.1. Flexera may transfer Personal Information outside of the territory in which it originates; where this occurs any such transfer is executed in accordance with Applicable Privacy Laws.

7.2. Where the processing Flexera entity is located outside the European Economic Area, the United Kingdom or Switzerland, the terms of the Standard Contractual Clauses annexed to Commission Implementing Decision (EU) 2021/914 (**"SCC"**), as further specified in Schedule 2 of this DPA, are hereby incorporated by reference and shall be deemed to have been executed by the parties and apply to any transfers of Personal Information falling within the scope of the European General Data Protection Regulation from Customer (as data exporter) to Flexera (as data importer). Schedule 2 will also specify the applicable module of the SCC.

7.3. To the extent that the processing of Personal Information is subject to data protection laws in the United Kingdom, Schedule 3 shall apply in addition.

8. Security of Personal Information

8.1. Flexera has in place a comprehensive data protection and information security program which consists of a range of technical and organisational measures designed to establish an appropriate level of security for all Personal Information processed by Flexera. The technical and organizational measure are specified in Annex 2 to Schedule 2.

8.2. All personnel of Flexera undergo appropriate pre-employment screening and are subject to written obligations of confidentiality extending to the Personal Information processed on behalf of Customer. Sub-processors will be bound by appropriate confidentiality agreements as well.

8.3. Flexera may alter the technical and organizational security measures provided that such alteration does not reduce the overall level of protection afforded to the Personal Information by Flexera under this Data Processing Agreement, it will inform Customer of any substantial changes

9. Requests for Information

9.1. Flexera has a policy in place for handling requests to access Personal Information it processes by third parties, including in respect of warrants, subpoenas, court orders, or requests from individuals or governmental departments (including law enforcement and intelligence agencies).

9.2. Flexera will notify Customer of such request on receipt unless there is a restriction on such notification. Where Flexera is prohibited from notifying Customer it shall provide such notification as soon as such restriction is no longer in effect.

9.3. Where Flexera receives such a request and is prohibited from notifying Customer, it shall use reasonable efforts to establish that the request is legitimate, is in accordance with applicable laws, and goes no further than is necessary to achieve the intended purpose.

9.4. Flexera has not received a request for information in respect of Personal Information it processes on behalf of its customers from any government, law enforcement, or intelligence agency.

10. Audit

10.1. Customer is entitled to audit Flexera's compliance with the obligations set out in this Data Processing Agreement including any Schedules were applicable once in any 12 months period, unless where an audit is recommended, or required by a regulator of Customer, following an Incident (as defined in Section 11 of this Data Processing Agreement), or where Customer has justifiable reason to believe that Flexera is not complying with the terms and conditions under this Data Processing Agreement.

10.2. Customer may conduct any audit itself or appoint a suitably qualified third party to conduct the audit on its behalf. Where Customer appoints a third party it agrees that it will not appoint any third party who provides comparable Services as Flexera, and that the third party must enter a written obligation of confidentiality approved by Flexera.

10.3. Any audit must be completed during Flexera's normal business hours and be conducted in such a manner as to prevent any unreasonable disruption or interference with Flexera's operations.

10.4. To initiate an audit Customer shall submit a comprehensive audit plan to Flexera no less than two weeks prior to the intended commencement date. Flexera will consider the request and shall work collaboratively with Customer to finalise the scope of the audit and seek to have the relevant resources available. Flexera shall use its reasonable endeavours to ensure that any third-party Sub-processors assist to the extent necessary with any such audit.

10.5. Where the intended scope of an audit is covered in an approved industry standard, scheme, or certification, Customer agrees to accept a certification of said standard issued by a third-party auditor or certification body within the preceding twelve months as confirmation of adherence to said standard, scheme, or certification.

10.6. Flexera and Customer shall each be responsible for their own costs in relation to, or arising from, the audit. In the event the Flexera is required to incur additional costs it shall notify Customer of the same prior to the audit commencing and both Flexera and Customer will negotiate in good faith with respect to any such costs.

11. Security Incident

11.1. Flexera has implemented and deployed a range of technical and organisational measures to minimise the risk of any unauthorised disclosure of or access to, and accidental or unlawful destruction, loss, alteration, or extraction of Personal Information (an "**Incident**"). The measures in question are intended to prevent an Incident occurring, identify if an Incident occurs, and minimise the impact if an Incident occurs.

11.2. Flexera will notify Customer without undue delay after becoming aware of an Incident. Flexera will provide the following information as it becomes available either at the time of notification or as soon as possible thereafter:

11.2.2. A description of the Incident,

11.2.3. Details of what Personal Information is affected,

11.2.4. What measures have been taken to mitigate the impact of the Incident,

11.2.5. If applicable, when access to the Personal Information will be restored.

11.3. Flexera will not make any public statement, notify any regulator, or notify the affected individuals without first notifying Customer. Customer agrees that it will coordinate with Flexera on the content and timing of any public statements or regulatory notifications that Customer intends to make in relation to the Incident.

12. Rights of Individuals

Flexera recognises there may be rights afforded to individuals under the Applicable Privacy Laws and has appropriate systems in place to enable such rights to be fulfilled within the stipulated timeframes. Where Flexera receives a request

for Personal Information and Flexera is processing such Personal Information at the direction of Customer, Flexera will forward the request on to Customer and may refer the individual making the request of the same to Customer. If Customer receives a request and requires Flexera's assistance to fulfil the request it shall forward the same to DataProtectionTeam@Flexera.com.

13. Data Erasure and Retention

In the absence of any provision within the Master Agreement to the contrary within sixty days of Flexera ceasing to provide the Services to Customer Flexera shall be hereby permitted to erase any Personal Information remaining on any of Flexera's systems.

14. Personal Information Subject to the CCPA

To the extent that the processing of Personal Information is subject to the California Consumer Privacy Act of 2018 ("**CCPA**"), Schedule 4 shall apply.

Schedule 1 – Data Processing

1. **Categories of Personal Information**:

   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. To the extent that the above items are not Personal Information, the provisions of this Data Processing Agreement (including the schedules) shall not be applicable.

2. **Categories of Individual**:

   Employees, contractors, agents, etc. of Customer

3. **Subject-matter, nature and purpose of Processing**:

   Providing the Services as agreed in the Master Agreement.

4. **Duration of Processing**:

   The duration shall correspond with the period of time for which the Services are provided and until all personal data is deleted according to Cl. 13.

5. **Approved Third Parties and Sub-Processors**:

   Flexera affiliates:

   - Flexera Software LLC – provides support, maintenance, and professional services
   - Flexera Software GmbH - providing professional services
   - Flexera Software Ltd- provides professional and maintenance services
   - Secunia ApS – provides IT security solutions alongside rendering support and maintenance services
   - Rightscale, Inc. – Provides cloud delivery solutions
   - Revulytics, Inc. – provides compliance intelligence services

   Third parties:

Akamai International B.V.	Amsterdam, Netherlands
Provides content delivery network services	
Akamai International Inc.	Massachusetts, USA
Provides content delivery network services	
GoodData Corporation	California, USA
Conducts analytic services as well as data platform services	
Intercom, Inc.	California, USA
Provides a communications platform	
Revulytics, Inc.	Massachusetts, USA
Provides compliance intelligence services	
Infinit-O Global Limited	Manila, Philippines
Provides business intelligence services	
Amazon Web Services (AWS)	Seattle, USA
Provides a cloud-based hosting platform	
Snowflake Inc.	Montana, USA
Provides a data warehousing service	

HCL, including • HCL America Inc. • HCL Technologies Limited • HCL Technologies Corporate Services Limited • HCL Mexico S. de R.L	 • California, USA • New Delhi, India • Surrey, UK • Jalisco, Mexico
Provides engineering, support and customer success services	

The Sub-Processors may have access to the Personal Information for the term of this Data Processing Agreement or until the service contract with the respective Sub-Processor is terminated or the access by the Sub-Processor has been excluded as agreed between Flexera and Customer.

Schedule 2 – EU/EEA Provisions & Standard Contractual Clauses

Applicable Module

For the purposes of data transfers between Customer and Flexera entities being primary processors and located outside the EEA, the United Kingdom or Switzerland, Module Two of the SCC – Controller to Processor - , shall apply and is hereby incorporated into this Schedule 2 as further specified below. Where the Flexera entities are located outside the EEA, the United Kingdom or Switzerland and process Personal Information from Customers who are processors, Module Three of the SCC - Processor to Subprocessor – shall apply and hereby be incorporated into this Schedule 2 as further specified below.

Elective Options

Docking Clause – Clause 7 The docking clause shall not apply
Appointment and use of Sub-processors - Clause 9(a) – option 2 is selected The time specified for Flexera to notify Customer of the intended appointment of a new Sub-processor is 28 days.
Independent dispute resolution body – Clause 11(a) The option to lodge complaints to an independent dispute resolution body shall not apply.
Governing law, jurisdiction and choice of forum - Clauses 17 – option 1 is selected – and 18(b) Where the Flexera contracting entity is Flexera GmbH the governing law will be that of Germany and the Courts of Germany shall have jurisdiction. Where the Flexera contracting entity is not Flexera GmbH the governing law will be that of Ireland and the Courts of Ireland shall have jurisdiction.

Annex 1 to Schedule 2

1. The Data Exporter

The Data Exporter is the Customer named in the Master Agreement. The Data Exporter's contact information is contained within the Master Agreement. Flexera may request the name and contact information of the, contact person, data protection officer (if applicable) and/or representative (if applicable) as well as the contact person's position at any time. The activities relevant to the data transferred are as described in the Master Agreement and the Main Body of the Data Processing Agreement. The Data Exporter is the Data Controller.

2. The Data Importer

The Data Importer is the Flexera entity named in the Master Agreement. The Data Importer's contact information is contained within the Master Agreement. Customer may request the name and contact information of the, contact person, data protection officer (if applicable) and/or representative (if applicable) at any time. The activities relevant to the data transferred are as described in the Master Agreement and the Main Body of the Data Processing Agreement. The Data Importer is a Data Processor.

3. Description of Transfer

The categories of data subjects, the Categories of Personal Information, the purpose of processing, and the sub-processors to which Personal Information is transferred are set out in Schedule 1 of this Data Processing Agreement. There will be no Sensitive data transferred. The transfer will be performed on a continuous basis during the term of the Master Agreement.

Where the data exporter is established in an EU Member State: The supervisory authority of the country in which the data exporter established is the competent authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of the GDPR: The competent supervisory authority is the one of the EU Member State in which the representative is established.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with its Article 3(2) without, however, having to appoint a representative pursuant to Article 27(2) of the GDPR: The competent supervisory authority shall be the supervisory authority in Ireland, namely the Data Protection Commission (https://www.dataprotection.ie/).

Annex 2

1. Description of the technical and organisational measures implemented by the data importer:

The Data Importer has a range of technical and organisational measures to minimise the risk to Personal Information and ensure ongoing confidentiality, integrity, availability, and resilience of processing systems including:

1.Pseudonymization and Encryption

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 such as: Physical access control systems; Definition of authorizes persons and Management and documentation of individual authorizations; Regulation of Visitors and external staff; Monitoring of all facilities housing IT systems; and Logging of physical access

2.1.2 System/Electronic access control

Measures that prevent data processing systems from being used without authorization, including: 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; and 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, including: Automatic and manual locking; 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, including: 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, including: Training and confidentiality agreements for internal staff and external staff

2.2Integrity

2.2.1Data 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, including: Secure transmission between client and server and to external systems by using industry-standard encryption; Secure network interconnections ensured by Firewalls etc.; and 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, including: Logging authentication and monitored logical system access; Logging of data access including, but not limited to access, modification, entry and deletion of data; and 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. These measures include: Tape-media based backup solution; Implementation of transport policies; Backup Concept and 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

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

Organizational measures that ensure the regular review and assessment of technical and organizational measures include: Testing of emergency equipment; Documentation of interfaces and personal data fields; and Internal assessments.

2. <u>For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter:</u>

Sub-processors engaged by Flexera will have a range of technical and organisational measures that offer an equivalent level of protection to the Personal Information that they process, these will be of a comparable nature to those described above.

Schedule 3 – United Kingdom Provisions and SCC Addendum

With respect to any transfers of Personal Information falling within the scope of the UK GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the UK European Union (Withdrawal) Act 2018 ("**UK GDPR**") from Customer (as data exporter) to Flexera (as data importer), the following shall apply:

1.1 The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 ("**Approved Addendum**") as further specified in this Schedule 3 shall form part of this Data Processing Agreement, and the SCC shall be read and interpreted in light of the provisions of the Approved Addendum, to the extent necessary according to Clause 12 lit. 1 of the Mandatory Clauses to the Approved Addendum ("**Mandatory Clauses**");

1.2 In deviation to Table 1 of the Approved Addendum and in accordance with Clause 17 of the Mandatory Clauses, the parties are further specified in Annex 1 to Schedule 2 of this Data Processing Agreement.

1.3 The selected Modules and Clauses to be determined according to Table 2 of the Approved Addendum are further specified in Schedule 2 of this Data Processing Agreement as amended by the Mandatory Clauses.

1.4 Annex 1 A to the Approved Addendum is specified by Annex 1 of this Data Processing Agreement and B of Table 3 to the Approved Addendum is specified by Schedule 1 of this Data Processing Agreement. Annex II of the Approved Addendum is specified by Annex 2 to Schedule 2 of this Data Processing Agreement, and Annex III of the Approved Addendum is specified by Schedule 1of this Data Processing Agreement.

1.5 Flexera (as data importer) may, to the extent the Approved Addendum applies, end this Data Processing Agreement in accordance with clause 19 of the Mandatory Clauses;

1.6 Clause 16 of the Mandatory Clauses shall not apply.

Schedule 4 – California Provisions

This schedule provides clarification as to the responsibilities of Flexera and Customer (each as defined in the Master Agreement) with regard to Personal Information originating from, or relating to, residents of California and subject to the CCPA. This Schedule shall only be effective where Customer is a Business as defined by the CCPA.

1. **Definitions**

"**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq., including any amendments and any implementing regulations thereto;

"**Consumer**" means a "consumer" as such term is defined in the CCPA;

"**Personal Information**" means the "personal information" (as defined in the CCPA) that Flexera Processes on behalf of the Customer in connection with the provision of the Services;

"**Sell**" and "**Sale**" have the meaning given in the CCPA; and

"**Services**" means the service(s) provided by Flexera to Customer under the Master Agreement

2. **Role of the Parties.** For the purposes of the CCPA, the Parties acknowledge and agree that Flexera will act as a "Service Provider" as such term is defined in the CCPA, in its performance of the Services.

3. **Instructions for Processing.** Flexera will retain, use and disclose the Personal Information for the purpose of performing the Services and otherwise only as permitted by the CCPA or as required by law.

4. **No Sale of Personal Information.** Flexera will not sell Personal Information to another business or third party for monetary or other valuable consideration.

5. **Access and Deletion.** Upon Customer's request and at Customer's reasonable expense, Flexera will assist customer with fulfilling requests to (or provide Customer with the ability to), delete, access or procure a copy of Personal Information.

6. **Certification of Compliance**. Flexera certifies that it understands the foregoing obligations and will comply with them.