SUSE DATA PROCESSING ADDENDUM (MLA/VLA)

(SUSE as Processor, Customer as Controller)

This Data Processing Addendum and its Attachments ("**DPA**") supplement, form an integral part of and are incorporated into any contract pursuant to which SUSE has agreed to provide Support Services, Consulting Services, Training Services or other services (collectively, the "**Services**") to a customer ("**Customer**") in connection with Customer's use of SUSE's software products (such contract, the "**Agreement**"), and reflects the Parties' agreement with respect to the Processing (as defined below) by SUSE of Customer Personal Data (as defined below). The Agreement will remain in full force and effect, except that it will be extended and modified as set forth in this DPA with respect to the activities contemplated in this DPA.

Unless otherwise agreed, the effective date of this DPA shall be the same as the effective date of the Agreement.

1. Definitions and Interpretation

1.1 Any capitalized terms not defined in this DPA will have the meanings set forth in the Agreement. In this DPA, unless the context requires otherwise:

"***Adequate Jurisdiction***" means the UK, EEA, or a country, territory, specified sector or international organisation which ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data, as set out in:

(a) with respect to Personal Data relating to Data Subjects in the EEA, a decision of the European Commission;

(b) with respect to Personal Data relating to Data Subjects in the UK, the UK Data Protection Act 2018 or regulations made by the UK Secretary of State under the UK Data Protection Act 2018.

"***Californian Data***" means Customer Personal Data that is subject to the protection of the CCPA.

"***CCPA***" means the California Consumer Privacy Act of 2018 as amended, including by the California Privacy Rights Act [1798.100 - 1798.199] and regulations adopted thereunder, as may be further amended, superseded or replaced.

"***Customer Personal Data***" means any Personal Data provided to SUSE by or on behalf of Customer and which SUSE Processes in connection with the Agreement, as further described in Attachment 1, Part A.

"***Data Protection Laws***" means all applicable laws, as may be amended, superseded or replaced, relating in any way to the privacy, confidentiality, data protection or security of personal data, including, without limitation, the GDPR and the UK GDPR.

"***European Data***" means Customer Personal Data that is subject to (i) the GDPR, (ii) the UK GDPR, and (iii) the Swiss FDPA.

"***European Economic Area***" or "***EEA***" means the Member States of the European Union together with Iceland, Norway, and Liechtenstein.

"***GDPR***" means Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) as may be amended, superseded or replaced.

"***Standard Contractual Clauses***" means the Standard Contractual Clauses annexed to Commission Implementing Decision (EU) 2021/914, a copy of which can be found at: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

"***Subprocessor***" means any processor engaged by SUSE who agrees to receive any Customer Personal Data from SUSE.

"***Swiss FDPA***" means the Swiss Federal Data Protection Act of 25 September 2020 and the Swiss Data Protection Ordinance as may be amended, superseded or replaced.

"***UK Addendum***" means the template Addendum issued by the UK Information Commissioner under s.119A of the UK Data Protection Act 2018 currently found at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf, as may be amended, superseded, or replaced.

"UK Data Protection Laws" means any laws relating to data protection, the Processing of Personal Data, privacy and/or electronic communications in force from time to time in the UK, including (but not limited to) the UK GDPR and the UK Data Protection Act 2018.

"UK GDPR" means the GDPR as it forms parts of the United Kingdom domestic law by virtue of Section 3 of the European Union (Withdrawal) Act 2018, as may be amended, superseded or replaced.

1.2 The terms "***Personal Data***", "***Personal Data Breach***", "***Controller***", "***Processor***", "***Data Subject***", and "***Process***" shall have the meanings given to them in the GDPR.

1.3 The term "***Party***" shall refer to SUSE and Customer individually and the term "***Parties***" shall refer to SUSE and Customer collectively.

1.4 In case of any conflict or inconsistency with the terms of the Agreement, the provisions of this DPA shall control regarding its subject matter.

2. Processing of Personal Data

2.1 **Roles of the Parties**. The Parties acknowledge and agree that with regard to the Processing of Customer Personal Data under the Agreement, Customer is a Controller and/or a Processor and SUSE is a Processor.

2.2 **Details of the Processing**. The duration of the Processing, the nature and purpose of the Processing, the types of Customer Personal Data Processed and the categories of Data Subjects for whom Customer Personal Data is Processed are set forth in Attachment 1, Part B to this DPA.

2.3 **Customer Responsibilities**: Customer acknowledges and agrees that:

(a) it will be solely responsible for (i) complying with all requirements that apply to it under applicable Data Protection Laws with respect to its Processing of Customer Personal Data and the instructions it issues to SUSE; (ii) the accuracy, quality, and legality of Customer Personal Data and the means by which it acquired Customer Personal Data; (iii) complying with all necessary transparency and lawfulness requirements under applicable Data Protection Laws for the collection and use of Customer Personal Data, including obtaining any necessary consents and authorizations (particularly for use for marketing purposes); and (iv) ensuring it has the right to transfer, or provide access to, Customer Personal Data to SUSE for Processing in accordance with the terms of the Agreement (including this DPA);

(b) it shall not share with, provide or make available to SUSE any Personal Data other than Customer Personal Data that is necessary in order for SUSE to perform the Services, and where the provision of Customer Personal Data is necessary for the provision of the Services, it shall take all reasonable steps to minimise the provision of such information, and to anonymise and/or pseudonymise such Customer Personal Data prior to it being provided or made available to SUSE; and

(c) it will inform SUSE without undue delay if it is not able to comply with its responsibilities under this Section 2.3 or applicable Data Protection Laws and will indemnify and hold harmless SUSE from and against any claims, liabilities, and damages to the extent due to Customer's breach of this Clause 2.3.

2.4 **SUSE Responsibilities**: SUSE acknowledges and agrees that:

(a) **Compliance with Instructions**: it shall only Process Customer Personal Data for the purposes described in this DPA or as otherwise agreed within the scope of Customer's lawful instructions, except where and to the extent otherwise required by applicable law, in which case it shall notify Customer of such legal requirements prior to Processing unless prohibited by such law on the grounds of an important public interest. Customer may issue further documented instructions throughout the duration of the Processing. SUSE will inform Customer without undue delay if it considers that any instructions given by Customer infringe any applicable Data Protection Laws. To the extent that any of Customer's instructions require processing of Customer Personal Data in a manner that falls outside the scope of the Services, SUSE may (i) make the performance of any such instructions subject to the payment by Customer of any costs and expenses incurred by SUSE or such additional charges as SUSE may reasonably determine; or (ii) if performance of any such instructions is impossible, terminate the Agreement and the Services on written notice, without liability to Customer.

(b) **Personnel:** only authorized personnel who have undergone appropriate training in the protection and handling of Personal Data and are bound in writing to respect the confidentiality of Customer Personal Data, have access to Customer Personal Data.

(c) **Security Measures**: 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, it shall implement and maintain appropriate technical and organizational measures to maintain the security, confidentiality and integrity of Customer Personal Data, including measures designed to protect Personal Data Breaches, and to ensure a level of security appropriate to the risk including, where applicable by virtue of Article 28(3)(c) of the GDPR, and as appropriate, the measures referred to in Article 32(1) of the GDPR. Without limiting the generality of the foregoing, SUSE shall implement and maintain the technical and organisational measures as set out in Attachment 1, Part C to this DPA ("**Security Measures**"). SUSE shall regularly test, assess and evaluate the effectiveness of the Security Measures to reasonably ensure the security of the Processing of Customer Personal Data. SUSE may, by written notice to Customer, vary the Security Measures, provided that such variation does not reduce the overall level of protection afforded to Customer Personal Data by SUSE under this DPA.

(d) **Reporting:** it shall make available to Customer on request all information necessary to demonstrate compliance with this DPA. In the event that Customer requests to conduct any audit under applicable Data Protection Laws, the Parties agree that (i) all such audits shall be conducted on reasonable written notice to SUSE, only during SUSE's normal business hours and in a manner that does not disrupt SUSE's business; and (ii) Customer (or, where applicable, a third party independent auditor appointed by Customer) shall enter into a confidentiality agreement with SUSE prior to conducting the audit in such form as SUSE may request, and ensure that its personnel comply with relevant SUSE's and any Subprocessor's policies and procedures, as notified to Customer by SUSE or Subprocessor.

(e) **Information Requests**: it shall promptly notify Customer if it receives a request from any Data Subject or data protection authority to conduct an audit or obtain further information about SUSE's Processing of Customer Personal Data under this DPA, and shall (i) unless required under applicable law, not respond to such request without Customer 's prior written consent, (ii) comply with any reasonable instructions provided by Customer with respect to such request, and (iii) provide reasonable assistance to Customer to respond to any such information request.

(f) **Data Protection Impact Assessment:** it shall, upon Customer's written request, provide reasonable assistance to Customer in connection with obligations under Articles 32 and 36 of the GDPR or equivalent provisions under applicable Data Protection Laws.

(g) **Deletion or Return of Personal Data**: it shall within 30 days of the date of termination or expiry of the Agreement, upon Customer's written request within that period, promptly destroy, anonymize or return any Customer Personal Data, unless storage of Customer Personal Data is required by applicable law.

2.5 **Costs**: Customer shall reimburse SUSE or Subprocessor for all reasonable costs and expenses incurred by SUSE or Subprocessor in the provision of support services in connection with clauses 2(e) to (g).

2.6 **Points of Contact**: if either party has any questions regarding Processing of Personal Data under the Agreement, it may send such questions to the relevant contact person(s) set out in Attachment 1, Part A.

3. Subprocessors

3.1 **Appointment of Subprocessors**. Customer acknowledges and agrees that SUSE may engage Subprocessors in connection with the fulfilment of its obligations under the Agreement. Customer grants SUSE general authorisation to engage any Subprocessors from an approved list, as set out in Attachment 1, Part D to this DPA (the "***Approved List***").

3.2 **Notification of New Subprocessors**. SUSE shall submit any notice of any intended change to the Approved List in writing at least thirty (30) days prior to the implementation of such change and shall provide any information reasonably necessary to enable Customer to determine whether to object to the change.

3.3 **Objection to New Sub-processors**. If Customer objects to any change to the Approved List on reasonable grounds, it shall provide SUSE with written notice of the objection within thirty (30) days after SUSE has

provided notice to Customer as described in Clause 3.2 above. SUSE will use reasonable endeavours to fulfil its obligations under the Agreement without implementing such change, failing which SUSE may terminate, with at least thirty (30) days written notice, the portion of the Services that requires the use of the Subprocessor to which the objection relates without liability to Customer.

4. Personal Data Breaches

4.1 **Personal Data Breach**. SUSE shall:

(a) notify Customer within forty-eight (48) hours of becoming aware of any Personal Data Breach;

(b) use its best efforts to recover and secure any Personal Data affected by the Personal Data Breach;

(c) provide Customer with periodic updates regarding the status of the Personal Data Breach as appropriate, taking into account the nature and circumstances of the Personal Data Breach;

(d) provide Customer with such reasonable assistance and cooperation as Customer may require in connection with any litigation or investigation brought by Customer against a third party in connection with the Personal Data Breach; and

(e) other than where required under applicable law, not notify any data subjects or supervisory authorities of the Personal Data Breach without Customer s prior written approval with respect to the timing, content, and method of such notification.

4.2 **Costs**. Customer shall reimburse SUSE for all reasonable costs and expenses incurred by SUSE in connection with a Personal Data Breach, except where such breach results from SUSE's breach of applicable Data Protection Laws or where it has acted outside of or contrary to the lawful instructions of Customer.

5. Data Transfers

5.1 Customer acknowledges and agrees that SUSE may transfer Customer Personal Data outside of the country from which it was originally collected, provided that such transfer is required in connection with the purpose of the Processing and such transfers take place in accordance with applicable Data Protection Laws, including, without limitation, completing any prior assessments required by Data Protection Laws.

6. Additional Provisions for European Data

The following additional provisions in this Section 6 will apply only with respect to European Data.

6.1 **International Transfers.** If Customer, in making use of the Services, is considered a "data exporter" and SUSE a "data importer", both within the meaning of Clause 1(1) of the Standard Contractual Clauses, the Parties agree that the Standard Contractual Clauses are incorporated by reference and form part of this DPA, as follows:

(a) if Customer is a Controller, Module Two (controller to processor) shall apply, and if Customer is a Processor, Module Three (processor to processor) shall apply;

(b) Clause 7 (Docking Clause) does not apply;

(c) the option in Clause 11(a) (Independent dispute resolution body) does not apply;

(d) with regard to Clause 17 (Governing law) and Clause 18 (Choice of forum and jurisdiction), the Parties agree that the governing law and the forum for disputes will be determined in accordance with Section 8.2; and

(e) the Annexes of the Standard Contractual Clauses shall be deemed to incorporate the information set out in the Attachments to this DPA.

To the extent that there is any conflict between this DPA and the Standard Contractual Clauses, the terms of the Standard Contractual Clauses shall prevail.

6.2 **Onward International Transfers**. Where SUSE transfers European Data, the Processing of which falls within the scope of the GDPR, to a country outside of the EEA that is not an Adequate Jurisdiction, SUSE can ensure compliance with Chapter V of the GDPR by using Standard Contractual Clauses, provided the conditions for their use are met.

6.3 **UK Data Transfers**. Where SUSE Processes European Data that is subject to the UK GDPR, all references to the Standard Contractual Clauses shall be read and interpreted in light of the provisions of the UK Addendum.

6.4 **Swiss Data Transfers.** Where SUSE Processes European Data that is subject to the Swiss FDPA, for all references to the Standard Contractual Clauses:

(a) references to "Regulation (EU) 2016/679" or "that Regulation" are replaced by "the Swiss FDPA";

(b) references to Regulation (EU) 2018/1725 shall be deemed deleted;

(c) references to the "Union", "EU" and "EU Member State" are all replaced with "Switzerland"; and

(d) references to the "competent supervisory authority" shall be to the Swiss Federal Data Protection and Information Commissioner.

7. Additional Provisions for Californian Data

The following additional provisions in this Section 7 will apply only with respect to Californian Data.

7.1 The Parties acknowledge and agree that Customer is a business and SUSE is a service provider for the purposes of the CCPA.

7.2 The Parties agree that SUSE will not Process Californian Data for any purpose other than as necessary for the specific purposes of the Processing as set out in Attachment 1, Part A of this DPA or as otherwise expressly permitted for service providers under the CCPA. In particular, SUSE will not sell or share Californian Data or combine it with any other personal data or information it collects (directly or via any other Party) other than as expressly permitted for service providers under the CCPA.

8. General Provisions

8.1 **Affiliates.** Customer acknowledges and agrees that all rights granted to Customer under this DPA are for the benefit of Customer and shall extend only to any Affiliate of Customer that has agreed to this DPA and executed a Participation Agreement pursuant to the terms of the Agreement.

8.2 **Governing Law and Jurisdiction.** Notwithstanding anything to the contrary in the Agreement, this DPA and the Standard Contractual Clauses shall be governed by, and construed in accordance with:

(a) to the extent that the EU GDPR applies to the processing of Customer Personal Data, the laws of Ireland;

(b) to the extent that the Swiss FDPA applies to the processing of Customer Personal Data, the laws of Switzerland; and

(c) in all other cases, the laws of England and Wales.

Notwithstanding the provisions of the Agreement as regards to this DPA and the Standard Contractual Clauses, the Parties submit themselves to the jurisdiction of the following courts:

(a) to the extent that the EU GDPR applies to the processing of Customer Personal Data, the courts of Ireland;

(b) to the extent that the Swiss FDPA applies to the processing of Customer Personal Data, the courts of Switzerland; and

(c) in all other cases, the courts of England and Wales.

8.3 **Limitation of Liability**. Any exclusions or limitations of liability set out in the Agreement shall apply to any losses suffered by either Party (whether in contract, tort (including negligence) or for restitution, or for breach of statutory duty or misrepresentation or otherwise) under this DPA other than to the extent such exclusion or limitation (a) limits the liability of the Parties to data subjects or (b) is not permitted by applicable law. SUSE shall not be liable for breach of this DPA to the extent such breach arises as a result of Customer's breach of its responsibilities as set out in clause 2.3 of this DPA.

ATTACHMENT 1

PART A – LIST OF THE PARTIES

Customer

Role: Controller and/or Processor

Name: As per the Agreement

Address: As per the Agreement

Company No: As per the Agreement

Contact details: As per the Agreement

SUSE

Role: Processor

Address: As per the Agreement

Company No: As per the Agreement

Contact details:

Contact: Data Protection Officer

Email: privacy@suse.com

PART B – DETAILS OF PROCESSING

1. **Categories of data subjects**

   The personal data transferred concern the following categories of data subjects:

   - *Business partners and vendors of Customer*
   - *Employees or contact persons of customers or Customer*
   - *Agents, advisors, contractors or users of Customer*

2. **Categories of personal data**

   Personal Data Processed by SUSE in the provision of the Services may include, but is not limited to the following categories of Personal Data:

   - *Registration information: name, company / employer, email, phone, title, position, security questions and answers;*
   - *Host and usage information: connection data, localisation data, session sequence number, session start and end times, session duration, logs of modifications made to customer system during Service, screencast of protocol;*
   - *Usability and platform stability: last sign-in, locale, terms acceptance, logfiles, IP address;*
   - *User-generated information: chat, free text, uploaded files*

3. **Special categories of personal data (if applicable)**

   None

4. **Frequency of the transfer**

   The frequency of Processing is continuous.

5. **Nature of the processing**

   Personal Data will be Processed in accordance with the Agreement (including this DPA) and may be subject to the following Processing activities: *Collection, recording, organisation, structuring, storage, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, restriction, erasure and destruction.*

6. **Purpose(s) of the data transfer and further processing**

   The purpose of the processing is:

   The provision of the Services, including:
   - *Creation and maintenance of accounts;*
   - *Allowing users to contact SUSE*
   - *Enabling user verification and login*
   - *Service personalisation*
   - *Monitor system security*
   - *Diagnose technical and security issues*
   - *Creation and maintenance of remote sessions*
   - *Maintain access and modification logs*
   - *Customer satisfaction surveys*

7. **Duration**

   Subject to Clause 2.4(g) of this DPA, the period for which Customer Personal Data will be retained will be for the duration of the Agreement, unless otherwise agreed.

8. **Subprocessors (if applicable)**

   See Attachment 1, Part D for additional detail in relation to Subprocessors.

9. **Competent Supervisory Authority**

   If the Standard Contractual Clauses and/or the UK Addendum apply, the supervisory authority that will act as competent supervisory authority will be determined in accordance with the Standard Contractual Clauses and/or the UK Addendum, as applicable.

PART C- SECURITY MEASURES

Description of the technical and organisational security measures implemented by SUSE in accordance with Clause 2.4(c) of this DPA:

At SUSE, we have defined information security roles and responsibilities. We have a dedicated cybersecurity team led by CISO/Head of Information Security responsible for the information security within the organization. Members of these teams are in several countries. This team closely cooperates with other teams within SUSE, including the legal department, compliance team, privacy team (including the data protection officer), and the team responsible for security of our products. This team relies on the best practices, stated in ISO 27001 and 27701, but also in other standards.

Certifications
SUSE has obtained various corporate wide security certifications, including for ISO 27001 (information security management system) and ISO 27701 (privacy information management system). Copies can be viewed here: https://www.suse.com/support/security/certifications/

Information Security Policy
At SUSE, we have a documented Information Security Policy that defines the security framework, security principles and protected entities, as well as classification scheme for information. This policy is regularly, at least once a year, reviewed. That applies to all our ISMS related policies.

Asset Management
IT assets at SUSE are managed and documented. The asset repository is regularly updated.

Personnel Security and Awareness
Background checks are conducted in accordance with applicable law. SUSE employees are required to follow the company's guidelines related to business ethics and confidentiality. Employees are bound by non-disclosure or confidentiality rules. All newly hired employees are required to complete mandatory security training and awareness are managed on a continuous basis.

Change Management
At SUSE, we control and manage changes to services and associated IT infrastructure components. SUSE established internal bodies to decide on the deployment of changes. Security evaluation is part of this decision-making process.

Third Party Security
At SUSE, we have measures in place to mitigate the risk that our suppliers would not be following applicable law or would have a low level of information security. We established an internal body and we have documented processes to promote the area of third-party security.

Vulnerability Management and Patch Management
At SUSE, we have a dedicated Vulnerability Management Policy. Vulnerability management helps us to discover previously unpatched and/or unmitigated system and application exploits. We have a formal process to monitor security vulnerabilities. The Vulnerability Management process is initiated and coordinated by the security team and includes 6 stages: preparation, communication, vulnerability assessment in SUSE products and internal SUSE systems, findings evaluation, remediation, and validation. Security patches and updates to applications, operating systems and network infrastructure are applicable to prevent the introduction of new vulnerabilities. We have a patch management program which includes specific timescales from patching based upon the criticality.

Authentication and Authorization
Access and Password Management Policy enforces requirements for authenticated access, basic password rules, locking-out access (accounts are locked after 5 unsuccessful attempts and an alert is raised), disclosing passwords and password storage, strong authentication (Multi Factor Authentication is used), privileged access, technical access, and system communication. The minimum length of a password must be 14 characters and consist of at least lowercase and uppercase letters. User passwords do not expire.

Software Development Lifecycle
At SUSE, we focus on how to manage development securely and effectively. Security is implemented during the whole software development lifecycle. SUSE has a dedicated security team for our products.

Incident Management
In case of an information security incident, SUSE has a documented Incident Management Process defining the major incident management steps, including identification, evaluation and closure. We also pay attention to communication of security incidents. We have a Crisis Communication team that is responsible for communicating internally and or externally all the security incidences.

Network Security
At SUSE, all entry and exit points are protected by at least one layer of firewalling. Wired LAN is completely isolated with no access to internal SUSE parts or DNS. Guest wireless is segregated by the firewall policies with no access to SUSE internal networks.

Physical Security
We have implemented a Physical Security Policy that enforces requirements for protecting SUSE physical information systems and includes standards for secure and safe operations. The physical security controls are implemented to our Data Centre, computer rooms or office space including fire detection systems, access control systems and cameras and CCTV.

Anti-virus and Anti-malware Protection
We utilize a state-of-the-art antivirus solution with automatic updating as well as a multi-layer defence-in-depth model to our anti-malware program across our environment.

PART D- APPROVED SUBPROCESSORS

Subprocessor	Location	Description of processing	Contact details
Okta, Inc	US	To provide identity management services enabling customers to create and maintain accounts.	privacy@okta.com
Salesforce, Inc	US	To provide customer relationship management software to SUSE.	privacy@salesforce.com
AWS, Inc	Germany	To provide computing software support to SUSE.	https://aws.amazon.com/privacy/
SAP (SAP Qualtrics)	Germany	To provide customer experience software support to SUSE.	https://www.qualtrics.com/privacy-statement/
Adobe, Inc (Marketo)	US	To provide marketing software support to SUSE.	https://www.adobe.com/privacy/policy.html
EPAM Systems Inc.	US	To facilitate the provision of the Services offered by SUSE to Partner and customers.	https://www.epam.com/privacy-policy
SUSE Affiliates from time to time	Various	To facilitate the provision of the Services offered by SUSE to Partner and customers.	privacy@suse.com