DATA PROCESSING AGREEMENT FOR LEANIX SUBSCRIPTION SERVICES

1. DEFINITIONS

1.1. "**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data; for the purposes of this DPA, where Customer acts as processor for another controller, it shall in relation to LeanIX be deemed as additional and independent Controller with the respective controller rights and obligations under this DPA.

1.2. "**Data Protection Law**" means the applicable legislation protecting the fundamental rights and freedoms of persons and their right to privacy with regard to the processing of Personal Data under the Agreement.

1.3. "**Data Subject**" means an identified or identifiable natural person as defined by Data Protection Law.

1.4. "**EEA**" means the European Economic Area, namely the European Union Member States along with Iceland, Liechtenstein and Norway.

1.5. "**GDPR**" means the General Data Protection Regulation 2016/679.

1.6. "**My Trust Center**" means information available on the SAP agreements website (see: https://www.sap.com/about/trust-center/agreements.html) or any subsequent website(s) made available by SAP to Customer.

1.7. "**EU SCC Relevant Transfer**" means a transfer (or an onward transfer) to a Third Country of Personal Data that is either subject to GDPR or to applicable Data Protection Law and where any required adequacy means under GDPR or applicable Data Protection Law can be met by entering into the EU Standard Contractual Clauses.

1.8. "**EU Standard Contractual Clauses**" means the unchanged standard contractual clauses, published by the European Commission, reference 2021/914 or any subsequent final version thereof which shall automatically apply. To avoid doubt Modules 2 and 3 shall apply as set out in Section 8.

1.9. "**Personal Data**" means any information relating to a Data Subject which is protected under Data Protection Law. For the purposes of the DPA, it includes only personal data which is:

a) entered by Customer or its Authorized Users into or derived from their use of the Subscription Service; or

b) supplied to or accessed by LeanIX or its Subprocessors in order to provide support under the Agreement. Personal Data is a sub-set of Customer Data (as defined under the Agreement).

1.10. "**Personal Data Breach**" means a confirmed:

a) accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or unauthorized third-party access to Personal Data; or

b) similar incident involving Personal Data, in each case for which a Controller is required under Data Protection Law to provide notice to competent data protection authorities or Data Subjects.

1.11. "**Processor**" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, be it directly as processor of a controller or indirectly as subprocessor of a processor which processes personal data on behalf of the controller.

1.12. "**Schedule**" means the numbered Annex with respect to the EU Standard Contractual Clauses.

1.13. "**Subprocessor**" or "**sub-processor**" means LeanIX Affiliates, SAP SE, SAP SE Affiliates and third parties engaged by LeanIX, SAP SE or SAP SE's Affiliates in connection with the Subscription Service and which process Personal Data in accordance with this DPA.

1.14. "**Technical and Organizational Measures**" means the technical and organizational measures for the relevant LeanIX Subscription Service published on My Trust Center (see: https://www.sap.com/about/trust-center/agreements/cloud/cloud-services.html?search=Technical%20Organizational%20Measures).

1.15. "**Third Country**" means any country, organization or territory not acknowledged by the European Union under Article 45 of GDPR as a safe country with an adequate level of data protection.

2. BACKGROUND

2.1. Purpose and Application

2.1.1. This document ("**DPA**") is incorporated into the Agreement and forms part of a written (including in electronic form) contract between LeanIX and Customer.

2.1.2. This DPA applies to Personal Data processed by LeanIX and its Subprocessors in connection with its provision of the Subscription Service.

2.1.3. This DPA does not apply to non-production environments of the Subscription Service if such environments are made available by LeanIX. Customer shall not store Personal Data in such environments.

2.2. Structure

Schedules 1 and 2 are incorporated into and form part of this DPA. They set out the agreed subject-matter, the nature and purpose of the processing, the type of Personal Data, categories of data subjects (Schedule 1) and the applicable Technical and Organizational Measures (Schedule 2).

2.3. Governance

2.3.1. LeanIX acts as a Processor and Customer and those entities that it permits to use the Subscription Service act as Controllers under the DPA.

2.3.2. Customer acts as a single point of contact and shall obtain any relevant authorizations, consents and permissions for the processing of Personal Data in accordance with this DPA, including, where applicable approval by Controllers to use LeanIX as a Processor. Where authorizations, consent, instructions or permissions are provided by Customer these are provided not only on behalf of the Customer but also on behalf of any other Controller using the Subscription Service. Where LeanIX informs or gives notice to Customer, such information or notice is deemed received by those Controllers permitted by Customer to use the Subscription Service. Customer shall forward such information and notices to the relevant Controllers.

3. SECURITY OF PROCESSING

3.1. Applicability of the Technical and Organizational Measures

LeanIX has implemented and will apply the Technical and Organizational Measures. Customer has reviewed such measures and agrees that as to the Subscription Service selected by Customer in the Order Form the measures are appropriate taking into account the state of the art, the costs of implementation, nature, scope, context and purposes of the processing of Personal Data.

3.2. Changes

3.2.1. LeanIX applies the Technical and Organizational Measures to LeanIX's entire customer base hosted out of the same data center or receiving the same Subscription Service. LeanIX may change the Technical and Organizational Measures at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

3.2.2. LeanIX will publish updated versions of the Technical and Organizational Measures on My Trust Center and where available Customer may subscribe to receive e-mail notification of such updated versions.

4. LEANIX OBLIGATIONS

4.1. Instructions from Customer

LeanIX will process Personal Data only in accordance with documented instructions from Customer. The Agreement (including this DPA) constitutes such documented initial instructions and each use of the Subscription Service then constitutes further instructions. LeanIX will use reasonable efforts to follow any other Customer instructions, as long as they are required by Data Protection Law, technically feasible and do not require changes to the Subscription Service. If any of the before-mentioned exceptions apply, or LeanIX otherwise cannot comply with an instruction or is of the opinion that an instruction infringes Data Protection Law, LeanIX will immediately notify Customer (email permitted).

4.2. Processing on Legal Requirement

LeanIX may also process Personal Data where required to do so by applicable law. In such a case, LeanIX shall inform Customer of that legal requirement before processing unless that law prohibits such information on important grounds of public interest.

4.3. Personnel

To process Personal Data, LeanIX and its Subprocessors shall only grant access to authorized personnel who have committed themselves to confidentiality. LeanIX and its Subprocessors will regularly train personnel having access to Personal Data in applicable data security and data privacy measures.

4.4. Cooperation

4.4.1. At Customer's request, LeanIX will reasonably cooperate with Customer and Controllers in dealing with requests from Data Subjects or regulatory authorities regarding LeanIX's processing of Personal Data or any Personal Data Breach.

4.4.2. If LeanIX receives a request from a Data Subject in relation to the Personal Data processing hereunder, LeanIX will promptly notify Customer (where the Data Subject has provided information to identify the Customer) via e-mail and shall not respond to such request itself but instead ask the Data Subject to redirect its request to Customer.

4.4.3. In the event of a dispute with a Data Subject as it relates to LeanIX's processing of Personal Data under this DPA, the Parties shall keep each other informed and, where appropriate, reasonably co-operate with the aim of resolving the dispute amicably with the Data Subject.

4.4.4. LeanIX shall provide functionality for production systems that supports Customer's ability to correct, delete or anonymize Personal Data from a Subscription Service, or restrict its processing in line with Data Protection Law. Where such functionality is not provided, LeanIX will correct, delete or anonymize any Personal Data, or restrict its processing, in accordance with the Customer's instruction and Data Protection Law.

4.5. Personal Data Breach Notification

LeanIX will notify Customer without undue delay after becoming aware of any Personal Data Breach and provide reasonable information in its possession to assist Customer to meet Customer's obligations to report a Personal Data Breach as required under Data Protection Law. LeanIX may provide such information in phases as it becomes available. Such notification shall not be interpreted or construed as an admission of fault or liability by LeanIX.

4.6. Data Protection Impact Assessment

If, pursuant to Data Protection Law, Customer (or its Controllers) are required to perform a data protection impact assessment or prior consultation with a regulator, at Customer's request, LeanIX will provide such documents as are generally available for the Subscription Service (for example, this DPA, the Agreement, Audit Reports and Certifications). Any additional assistance shall be mutually agreed between the Parties.

5. DATA EXPORT AND DELETION

5.1. Export and Retrieval by Customer

During the Subscription Term and subject to the Agreement, Customer can access its Personal Data at any time. Customer may export and retrieve its Personal Data in a standard format. Export and retrieval may be subject to technical limitations, in which case LeanIX and Customer will find a reasonable method to allow Customer access to Personal Data.

5.2. Deletion

Before the Subscription Term expires, Customer may use LeanIX's self-service export tools (as available) to perform a final export of Personal Data from the Subscription Service (which shall constitute a "return" of Personal Data). At the end of the Subscription Term, Customer hereby instructs LeanIX to delete the Personal Data remaining on servers hosting the Subscription Service within a reasonable time period in line with Data Protection Law (not to exceed 6 months) unless applicable law requires retention.

6. CERTIFICATIONS AND AUDITS

6.1. Customer Audit

Customer or its independent third party auditor reasonably acceptable to LeanIX (which shall not include any third party auditors who are either a competitor of LeanIX or not suitably qualified or independent) may audit LeanIX's control environment and security practices relevant to Personal Data processed by LeanIX only if:

a) LeanIX has not provided sufficient evidence of its compliance with the Technical and Organizational Measures that protect the production systems of the Subscription Service through providing either: (i) a certification as to compliance with ISO 27001 or other standards (scope as defined in the certificate); or (ii) a valid ISAE3402 or ISAE3000 or other SOC1-3 attestation report. Upon Customer's request audit reports or ISO certifications are available through the third party auditor or LeanIX;

b) a Personal Data Breach has occurred;

c) an audit is formally requested by Customer's data protection authority; or

d) provided under mandatory Data Protection Law conferring Customer a direct audit right and provided that Customer shall only audit once in any 12 month period unless mandatory Data Protection Law requires more frequent audits.

6.2. Other Controller Audit

Any other Controller may assume Customer's rights under Section 6.1 only if it applies directly to the Controller and such audit is permitted and coordinated by Customer. Customer shall use all reasonable means to combine audits of multiple other Controllers to avoid multiple audits unless the audit must be undertaken by the other Controller itself under Data Protection Law. If several Controllers whose Personal Data is processed by LeanIX on the basis of the Agreement require an audit, Customer shall use all reasonable means to combine the audits and to avoid multiple audits.

6.3. Scope of Audit

Customer shall provide at least 60 days advance notice of any audit unless mandatory Data Protection Law or a competent data protection authority requires shorter notice. The frequency and scope of any audits shall be mutually agreed between the parties acting reasonably and in good faith. Customer audits shall be limited in time to a maximum of 3 business days. Beyond such restrictions, the parties will use current certifications or other audit reports to avoid or minimize repetitive audits. Customer shall provide the results of any audit to LeanIX.

6.4. Cost of Audits

Customer shall bear the costs of any audit unless such audit reveals a material breach by LeanIX of this DPA, then LeanIX shall bear its own expenses of an audit. If an audit determines that LeanIX has breached its obligations under the DPA, LeanIX will promptly remedy the breach at its own cost.

7. SUBPROCESSORS

7.1. Permitted Use

LeanIX is granted a general authorization to subcontract the processing of Personal Data to Subprocessors, provided that:

a) LeanIX or SAP SE on its behalf shall engage Subprocessors under a written (including in electronic form) contract consistent with the terms of this DPA in relation to the Subprocessor's processing of Personal Data. LeanIX shall be liable for any breaches by the Subprocessor in accordance with the terms of this Agreement;

b) LeanIX will evaluate the security, privacy and confidentiality practices of a Subprocessor prior to selection to establish that it is capable of providing the level of protection of Personal Data required by this DPA; and

c) LeanIX's list of Subprocessors in place on the effective date of the Agreement is published by LeanIX on the following website https://www.leanix.net/en/legal/list-of-subprocessorsor a replacement website as made available by LeanIX to Customer or LeanIX will make it available to Customer upon request,

including the name, address and role of each Subprocessor LeanIX uses to provide the Subscription Service.

7.2. New Subprocessors

LeanIX's use of Subprocessors is at its discretion, provided that:

a) LeanIX will inform Customer in advance of any intended additions or replacements to the list of Subprocessors including name, address and role of the new Subprocessor by notifying the contacts provided by Customer on https://www.leanix.net/en/legal/list-of-subprocessors. Customer shall be responsible to maintain such contact up to date; and

b) Customer may object to such changes as set out in Section 7.3.

7.3. Objections to New Subprocessors

7.3.1. If Customer has a legitimate reason under Data Protection Law to object to the new Subprocessors' processing of Personal Data, Customer may terminate the Agreement (limited to the Subscription Service for which the new Subprocessor is intended to be used) on written notice to LeanIX. Such termination shall take effect at the time determined by the Customer which shall be no later than 30 days from the date of LeanIX's notice to Customer informing Customer of the new Subprocessor. If Customer does not terminate within this 30 day period, Customer is deemed to have accepted the new Subprocessor.

7.3.2. Within the 30 day period from the date of LeanIX's notice to Customer informing Customer of the new Subprocessor, Customer may request that the parties discuss in good faith a resolution to the objection. Such discussions shall not extend the period for termination and do not affect LeanIX's right to use the new Subprocessor(s) after the 30 day period.

7.3.3. Any termination under this Section 7.3 shall be deemed to be without fault by either party and shall be subject to the terms of the Agreement.

7.4. Emergency Replacement

LeanIX may replace a Subprocessor without advance notice where the reason for the change is outside of LeanIX's reasonable control and prompt replacement is required for security or other urgent reasons. In this case, LeanIX will inform Customer of the replacement Subprocessor as soon as possible following its appointment. Section 7.2 applies accordingly.

8. INTERNATIONAL PROCESSING

8.1. Conditions for International Processing

LeanIX shall be entitled to process Personal Data, including by using Subprocessors, in accordance with this DPA outside the country in which the Customer is located as permitted under Data Protection Law.

8.2. Applicability of EU Standard Contractual Clauses

8.2.1. The following shall apply in respect of EU SCC Relevant Transfers:

8.2.1.1. Where LeanIX is not located in a Third Country and acts as a data exporter, LeanIX (or SAP SE on its behalf) has entered in to the EU Standard Contractual Clauses with each Subprocessor as the data importer. Module 3 (Processor to Processor) of the EU Standard Contractual Clauses shall apply to such EU SCC Relevant Transfers.

8.2.1.2. Where LeanIX is located in a Third Country:

LeanIX and Customer hereby enter into the EU Standard Contractual Clauses with Customer as the data exporter and LeanIX as the data importer which shall apply as follows:

a) Module 2 (Controller to Processor) shall apply where Customer is a Controller; and

b) Module 3 (Processor to Processor) shall apply where Customer is a Processor. Where Customer acts as Processor under Module 3 (Processor to Processor) of the EU Standard Contractual Clauses, LeanIX acknowledges that Customer acts as Processor under the instructions of its Controller(s).

8.2.2. Other Controllers or Processors whose use of the Subscription Services has been authorized by Customer under the Agreement may also enter into the EU Standard Contractual Clauses with LeanIX in the same manner as Customer in accordance with Section 8.2.1.2 above. In such case, Customer enters into the EU Standard Contractual Clauses on behalf of the other Controllers or Processors.

8.2.3. With respect to a EU SCC Relevant Transfer, on request from a Data Subject to the Customer, Customer may make a copy of Module 2 or 3 of the EU Standard Contractual Clauses entered into between Customer and LeanIX (including the relevant Schedules), available to Data Subjects.

8.2.4. The governing law of the EU Standard Contractual Clauses shall be the law of Germany.

8.3. Relation of the EU Standard Contractual Clauses to the Agreement

Nothing in the Agreement shall be construed to prevail over any conflicting clause of the EU Standard Contractual Clauses. For the avoidance of doubt, where this DPA further specifies audit and Subprocessor rules, such specifications also apply in relation to the EU Standard Contractual Clauses.

8.4. Third Party Beneficiary Right under the EU Standard Contractual Clauses

8.4.1. Where Customer is located in a Third Country and acting as a data importer under Module 2 or Module 3 of the EU Standard Contractual Clauses and LeanIX is acting as Customer's sub-processor under the applicable Module, the respective data exporter shall have the following third party beneficiary right:

8.4.2. In the event that Customer has factually disappeared, ceased to exist in law or has become insolvent (in all cases without a successor entity that has assumed the legal obligations of the Customer by contract or by operation of law), the respective data exporter shall have the right to terminate the affected Subscription Service

solely to the extent that the data exporter's Personal Data is processed. In such event, the respective data exporter also instructs LeanIX to erase or return the Personal Data.

9. DOCUMENTATION; RECORDS OF PROCESSING

9.1. Each party is responsible for its compliance with its documentation requirements, in particular maintaining records of processing where required under Data Protection Law. Each party shall reasonably assist the other party in its documentation requirements, including providing the information the other party needs from it in a manner reasonably requested by the other party (such as using an electronic system), in order to enable the other party to comply with any obligations relating to maintaining records of processing.

Schedule 1 Description of the Processing

This Schedule 1 applies to describe the Processing of Personal Data for the purposes of the EU Standard Contractual Clauses and applicable Data Protection Law.

1. A. LIST OF PARTIES

1.1. Under the EU Standard Contractual Clauses

1.1.1. Module 2: Transfer Controller to Processor

Where LeanIX is located in a Third Country, Customer is the Controller and LeanIX is the Processor, then Customer is the data exporter and LeanIX is the data importer.

1.1.2. Module 3: Transfer Processor to Processor

Where LeanIX is located in a Third Country, Customer is a Processor and LeanIX is a Processor, then Customer is the data exporter and LeanIX is the data importer.

2. B. DESCRIPTION OF TRANSFER

2.1. Data Subjects

Unless provided otherwise by the data exporter, transferred Personal Data relates to the following categories of Data Subjects: employees, contractors, business partners or other individuals having Personal Data stored in the Subscription Service, transmitted to, made available to, accessed or otherwise processed by the data importer.

2.2. Data Categories

The transferred Personal Data concerns the following categories of data:

Customer determines the categories of data per Subscription Service subscribed. Customer can configure the data fields during implementation of the Subscription Service or as otherwise provided by the Subscription Service. The transferred Personal Data typically relates to the following categories of data: name, phone numbers, e-mail address, address data, system access / usage / authorization data, company name, contract data, invoice data, plus any application-specific data that Authorized Users enter into the Subscription Service and may include bank account data, credit or debit card data.

2.3. Special Data Categories (if agreed)

2.3.1. The transferred Personal Data may comprise special categories of personal data set out in the Agreement ("**Sensitive Data**"). LeanIX has taken Technical and Organizational Measures as set out in Schedule 2 to ensure a level of security appropriate to protect also Sensitive Data.

2.3.2. The transfer of Sensitive Data may trigger the application of the following additional restrictions or safeguards if necessary to take into consideration the nature of the data and the risk of varying likelihood and severity for the rights and freedoms of natural persons (if applicable):

a) training of personnel;

b) encryption of data in transit and at rest;

c) system access logging and general data access logging.

2.3.3. In addition, the Subscription Services provide measures for handling of Sensitive Data as described in the Documentation.

2.4. Purposes of the data transfer and further processing; Nature of the processing

2.4.1. The transferred Personal Data is subject to the following basic processing activities:

a) use of Personal Data to set up, operate, monitor and provide the Subscription Service (including operational and technical support);

b) continuous improvement of service features and functionalities provided as part of the Subscription Service including automation, transaction processing and machine learning;

c) provision of embedded Professional Services;

d) communication to Authorized Users;

e) storage of Personal Data in dedicated data centers (multi-tenant architecture);

f) release, development and upload of any fixes or upgrades to the Subscription Service;

g) back up and restoration of Personal Data stored in the Subscription Service;

h) computer processing of Personal Data, including data transmission, data retrieval, data access;

i) network access to allow Personal Data transfer;

j) monitoring, troubleshooting and administering the underlying Subscription Service infrastructure and database;

k) security monitoring, network-based intrusion detection support, penetration testing; and

l) execution of instructions of Customer in accordance with the Agreement.

2.4.2. The purpose of the transfer is to provide and support the Subscription Service. LeanIX and its Subprocessors may support the Subscription Service data centers remotely. LeanIX and its Subprocessors provide support when a Customer submits a support ticket as further set out in the Agreement.

2.5. Additional description in respect of the EU Standard Contractual Clauses:

2.5.1. Applicable Modules of the EU Standard Contractual Clauses

a) Module 2: Transfer Controller to Processor

b) Module 3: Transfer Processor to Processor

2.5.2. For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

In respect of the EU Standard Contractual Clauses, transfers to Subprocessors shall be on the same basis as set out in the DPA.

2.5.3. The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Transfers shall be made on a continuous basis.

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

determine that period.

Personal Data shall be retained for the duration of the Agreement and subject to Section 5.2 of the DPA.

3. C. COMPETENT SUPERVISORY AUTHORITY

3.1. In respect of the EU Standard Contractual Clauses:

3.1.1. Module 2: Transfer Controller to Processor

3.1.2. Module 3: Transfer Processor to Processor

3.2. Where Customer is the data exporter, the supervisory authority shall be the competent supervisory authority that has supervision over the Customer in accordance with Clause 13 of the EU Standard Contractual Clauses.

Schedule 2 Technical and Organizational Measures

This Schedule 2 applies to describe the applicable technical and organizational measures for the purposes of the EU Standard Contractual Clauses and applicable Data Protection Law.

LeanIX will apply and maintain the Technical and Organizational Measures.

To the extent that the provisioning of the Subscription Service comprises EU SCC Relevant Transfers, the Technical and Organizational Measures set out in Schedule 2 describe the measures and safeguards which have been taken to fully take into consideration the nature of the personal data and the risks involved. If local laws may affect the compliance with the clauses, this may trigger the application of additional safeguards applied during transmission and to the processing of the personal data in the country of destination (if applicable: encryption of data in transit, encryption of data at rest, anonymization, pseudonymization).