Data Processing Agreement

1 General

This **Data Processing Agreement** (hereinafter “**DPA**”) applies to the offering provided by the **Checkmk GmbH**, Kellerstraße 27, 81667 Munich, Germany (**“Provider”**) to the Customer based on the Subscription Agreement regarding the provision of Checkmk Cloud (SaaS) and Checkmk OEM Support for Checkmk Cloud (SaaS) and Checkmk Software (Self-Hosted). The DPA shall apply as of the effective date of the applicable Subscription Agreement.

2 Definitions

All terms defined elsewhere in the Subscription Agreement apply mutatis mutandis to this DPA. In addition, the following definitions apply:

2.1 “**Business Operations**” means such Personal Data processing activities where the Customer and the Provider agree that the Provider may carry out for its own internal purposes.

2.2 **“Checkmk Cloud (SaaS)”** means the Provider’s software-as-a-service offering, including Checkmk OEM Support Services with the functionalities and features defined in the respective Checkmk Cloud Edition (SaaS), which the Customer has licensed in accordance with the Subscription Agreement, as described in more detail in the User Guide Cloud (SaaS) and updated from time to time.

2.3 **“Checkmk OEM Support”** means the support services provided by the Provider under a Subscription Agreement for Checkmk Software (Self-Hosted) or Checkmk Cloud (SaaS) in accordance with the **“Service Description Checkmk OEM Support and SLAs”**. The most recent version of the **Service Description Checkmk OEM Support and SLAs** is available and can be accessed at https://checkmk.com/legal/support.

2.4 **“Checkmk Software (Self-Hosted)”** means the Provider’s self-hosting offering, including Checkmk OEM Support Services, with the functionalities and features defined in the respective Checkmk Software Edition (Self-Hosted), which the Customer has licensed in accordance with the Subscription Agreement, as described in more detail in the User Guide Software (Self-Hosted) and updated from time to time.

2.5 "**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.

2.6 "**Data Protection Law**" means the applicable legislation, in multiple jurisdictions worldwide, that relate to (i) protecting the fundamental rights and freedoms of persons and their right to privacy with regard to the processing of Personal Data under the Subscription Agreement; or (ii) protecting, securing, processing, transferring, storing or preventing unauthorized access to Personal Data. Data Protection Law includes, as far as it concerns the relationship between the parties regarding the processing of Personal Data by the Provider, the GDPR as a minimum standard, irrespective of whether the Personal Data is subject to GDPR or not.

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

2.8 "**EEA**" means the European Economic Area, namely the European Union member states along with Iceland, Liechtenstein and Norway.

2.9 "**EU**" means the European Union.

2.10 "**Personal Data**" means any information relating to a natural person that is subject to Data Protection Law. For the purposes of this DPA, it includes only personal data which is (i) entered by the Customer into or derived from their use of Checkmk Cloud (SaaS); or (ii) in the context of Premium Support or (iii) processed in the context of Checkmk OEM Support, which includes personal data in the support systems used for this purpose as soon as these are provided by the Processor in a cloud environment; or (iv) supplied to or accessed by the

Provider and/or its Sub-processors in order to provide any additional services under the Subscription Agreement (as set out in the Subscription Agreement).

2.11 "**Personal Data Breach**" means a confirmed (i) accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or unauthorized third-party access to Personal Data; or (ii) similar incident involving Personal Data, in each case for which the Customer is required under Data Protection Law to provide notice to competent data protection authorities and/or Data Subjects.

2.12 "**Processor**" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of its client, be it directly as the processor of a client or indirectly as sub-processor of the processor which processes personal data on behalf of the client.

2.13 "**Sub-processor**" means the Provider's Affiliates and third parties engaged by the Provider in connection with Checkmk Cloud (SaaS) and/or Checkmk OEM Support and which process Personal Data in accordance with this DPA.

3 Structure

3.1 The Provider will process Personal Data as Processor on behalf of the Customer as Controller, except where the Provider processes Personal Data carrying out its Business Operations in which case the Provider acts as Controller (this concerns the processing of Service Generated Data for the purposes of performance analysis and improvement of Checkmk Cloud (SaaS) and Checkmk Software (Self-Hosted) in accordance with the regulations set out in the Terms and Conditions for Checkmk Software (Self-Hosted) and Checkmk Cloud (SaaS) https://checkmk.com/legal/terms-and-conditions).

3.2 The parties agree that it is each party's responsibility to review and adopt requirements imposed on controllers and processors by the GDPR.

3.3 The **Schedule** to this DPA is incorporated into and forms part of this DPA. It sets out the agreed subject-matter, the nature and purpose of the processing, the type of Personal Data and categories of Data Subjects.

4 Security of processing

4.1 Appropriate technical and organizational measures: The Provider has implemented and will apply appropriate technical and organizational measures throughout the term of the Subscription Agreement (as set out at https://checkmk.com/legal/toms as of the Effective Date).

4.2 Changes: The Provider may change the implemented measures (as set out at https://checkmk.com/legal/toms as of the Effective Date) 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.

5 The Provider's obligations

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

5.2 Processing on legal requirement: The Provider may also process Personal Data where required to do so by applicable EU or member state law. In such a case, the Provider will inform the Customer of that legal requirement before processing unless that law prohibits such information on important grounds of public interest.

5.3 Personnel: To process Personal Data, the Provider and its Sub-processors will only grant access to authorized personnel who have committed themselves to confidentiality. The

Provider and its Sub-processors will regularly train personnel having access to Personal Data in applicable data security and data privacy measures.

5.4 Cooperation: At the Customer's request, the Provider will reasonably cooperate with the Customer in dealing with requests from Data Subjects or regulatory authorities regarding the Provider's processing of Personal Data or any Personal Data Breach. The Provider will promptly and in any event not later than reasonably required under applicable Data Protection Law, notify the Customer as soon as reasonably practical about any request it has received from a Data Subject in relation to the Personal Data processing, without itself responding to such request without the Customer's further instructions, if applicable. The Provider will provide functionality that supports the Customer's ability to correct or remove Personal Data from Checkmk Cloud (SaaS) and/or the systems for the provision of Checkmk OEM Support or block access to or restrict its processing in line with Data Protection Law. Where such functionality is not provided, the Provider will correct or remove any Personal Data or block access to or restrict its processing, in accordance with the Customer's instruction and Data Protection Law; apart from this, the Customer may also access its Personal Data at any time during the term of the Subscription Agreement. The Provider may upon mutual agreement between the parties, provide other information and reasonable assistance as may be required – beyond sentence 1 of this section 5.4 of this DPA or the purpose of responding to any such Data Subjects or otherwise to comply with duties under applicable Data Protection Law.

5.5 Personal Data Breach notification: The Provider will notify the Customer without undue delay if required by Data Protection Law, after becoming aware of any Personal Data Breach and provide reasonable information in its possession regarding the Personal Data Breach to assist the Customer to report a Personal Data Breach as the Provider is required to under Data Protection Law; other assistance may be provided upon mutual agreement. The Provider may provide such information in phases as it becomes available. Such notification must not be interpreted or construed as an admission of fault or liability by the Provider. Unless required by Data Protection Law, the Provider will not inform any third party of any Personal Data Breach without first obtaining the Customer’s prior consent at least in text form.

5.6 Data protection impact assessment: If, pursuant to Data Protection Law, the Customer is required to perform a data protection impact assessment or prior consultation with a regulator, at the Customer's request, the Provider will provide such documents as are generally available for Checkmk Cloud (SaaS) and/or Checkmk OEM Support (e.g., this DPA, the GTC, audit reports or certifications). Any additional assistance will be mutually agreed between the parties.

6 Data return and deletion

Upon termination of the Subscription Agreement, the Customer must instruct the Provider whether the Personal Data should be deleted or returned to the Customer (i.e., by means of a technical export, which will constitute a “return”) in accordance with Data Protection Law. Following such return or deletion, the Provider will retain Personal Data only if and to the extent required under EU or member state law. If the Customer fails to provide such instructions, the Provider will retain the relevant Personal Data for a reasonable period of time and then delete it.

7 Audits

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

7.1.1 the Provider has not provided sufficient evidence of its compliance with the technical and organizational measures that protect the systems of Checkmk Cloud (SaaS) and/or Checkmk OEM Support 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 and/or ISAE3000 or other SOC1-3 attestation report. Upon the Customer's request audit reports or ISO certifications are available through the third-party auditor or the Provider;

7.1.2 a Personal Data Breach has occurred;

7.1.3 an audit is formally requested by the Customer's data protection authority; or

7.1.4 Data Protection Law provides Customer with a direct audit right and provided that Customer will only audit once in any twelve (12) month period unless Data Protection Law requires more frequent audits.

7.2 Further requirements: Audits of the Provider's control environment and security practices relevant to the Customer's Personal Data processed by the Provider under this DPA are subject to the condition that it can be technically ensured that during an audit no access can be gained to data that is not processed within the scope of the Subscription Agreement with the Customer and in particular to data of other customers of the Provider. The Provider may refuse to provide information or access to the Provider's business premises and IT systems if and to the extent that this could violate confidentiality obligations of the Provider. The Provider makes available to the Customer all information necessary to demonstrate compliance with its obligations which are hereby agreed upon.

7.3 Scope of audit: Except in the event of a Personal Data Breach, the Customer will provide at least sixty (60) days advance notice of any audit unless mandatory Data Protection Law or a competent data protection authority requires shorter notice (or sooner if mutually agreed upon by the parties). The Customer audits will be limited in time to a maximum of three (3) business days, unless otherwise agreed to between the parties. The Customer will provide the results of any audit to the Provider.

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

8 Sub-processors

8.1 Permitted use: The Provider is granted a general authorization to subcontract the processing of Personal Data to Sub-processors, as follows:

8.1.1 The Provider will engage Sub-processors under a written (including in electronic form) contract consistent with the terms of this DPA in relation to the Sub-processor's processing of Personal Data and the Provider will be fully liable for any breaches by and all acts and omissions of its Sub-processors in accordance with this DPA.

8.1.2 The Provider will exercise appropriate due diligence in selecting Sub-processors and will evaluate the security, privacy and confidentiality practices of a Sub-processor prior to selection to establish that it is capable of providing the level of protection of Personal Data required by this DPA and the Provider will regularly evaluate each Sub-processor's security practices as they relate to data handling.

8.1.3 The Customer authorizes the Provider to subcontract the Sub-processors to provide Checkmk Cloud (SaaS) and/or Checkmk OEM Support (as listed at https://checkmk.com/legal/sub-processors as of the Effective Date, including the name, location of processing and role of each Sub-processor).

8.2 New Sub-processors: The Provider will update the list of Sub-processors (as listed at https://checkmk.com/legal/sub-processors) when appointing a new Sub-processor, including name, location of processing and role of the new Sub-processor. Customers can automatically be notified of changes to Sub-processors by subscribing to receive Trust Center notifications at https://trust.checkmk.com/#subprocessors. The Customer may object to such changes as set out in section 8.3 of this DPA below.

8.3 Objections to new Sub-processors: The Customer may object to any new proposed Sub-processors as follows:

8.3.1 If the Customer has a legitimate reason to object to the new Sub-processors' processing of Personal Data, the Customer may terminate the Subscription Agreement for which the new Sub-processor is intended to be used on written notice to the Provider (text form being sufficient). Such termination will take effect at the time determined by the Customer which will be no later than fourteen (14) days from the date of the Provider's notice to the Customer informing the Customer of the new Sub-processor. If the Customer does not terminate within this fourteen (14) day period, the Customer is deemed to have accepted the new Sub-processor.

8.3.2 Within the fourteen (14) day period from the date of the Provider's notice to the Customer informing the Customer of the new Sub-processor, the Customer may request that the parties come together in good faith to discuss a resolution to the objection. Such discussions will not extend the period for termination and do not affect the Provider's right to use the new Sub-processor(s) after the fourteen (14) day period.

8.3.3 Any termination under this in section 8.3 of this DPA will be deemed to be without fault by either party and will be subject to the terms of the Subscription Agreement; provided, that no fee or penalty will be payable by the Customer in connection with such termination.

8.4 Emergency replacement: The Provider may replace a Sub-processor without advance notice where the reason for the change is outside of the Provider's reasonable control and prompt replacement is required for security or other urgent reasons, subject to sections 8.1.1 and 8.1.2 of this DPA above. In this case, the Provider will inform the Customer of the replacement Sub-processor as soon as possible following its appointment. Section 8.3 of this DPA applies accordingly.

9 International processing

The Provider is authorized to transfer Personal Data to countries outside the EU/EEA. If Personal Data is processed under the Subscription Agreement and this DPA is transferred from a country within the EU/EEA to a country outside the EU/EEA, the parties will ensure that the Personal Data is adequately protected. To achieve this, the Provider will, unless agreed otherwise, only transfer Personal Data outside the EU/EEA in accordance with the requirements of chapter V of the GDPR.

10 Documentation; records of processing

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 will 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 under Data Protection Law relating to maintaining records of processing. The Provider will make such records available to the Customer or a supervisory authority upon request, both in accordance with Data Protection Law.

Schedule to this DPA:

Schedule – Details of the Data Processing

Schedule – Details of the Data Processing

Description	Details
Categories of Data Subjects	**Checkmk Cloud (SaaS)** The Data Subjects include (i) users authorized by the Customer to use Checkmk Cloud (SaaS) and (ii) users of monitored systems as determined at the Customer's sole discretion. **Checkmk OEM Support for Checkmk Cloud (SaaS) or Checkmk Software (Self-Hosted)** Data subjects include users authorized by the Customer who provide personal data of the Customer or third parties in connection with Checkmk OEM Support within the support systems used for this purpose, as soon as these support systems are provided by the Processor in a cloud environment. **Premium Support** Data subjects include (i) users authorized by the Customer who make use of Live Support with Premium Support services and (ii) personal data of the Customer or third parties potentially disclosed by the Customer under its own responsibility in connection with Premium Support. Premium Support is described in the Service Description Checkmk OEM Support and SLAs.
Categories of Personal Data	**Checkmk Cloud (SaaS), Checkmk OEM Support for Checkmk Cloud (SaaS) or Checkmk Software (Self-Hosted)** - The Customer is required to provide certain Personal Data in order to use Checkmk Cloud (SaaS) (including master data such as first and last name, job title, telephone number, address and email addresses of End Users and (Premium) Support Contacts. - Data required for client authorization (including names of End Users, email addresses, permission roles of specific administrators and/or end-users as well as access credentials). - Client log files and application log files related to the use of Checkmk Cloud (SaaS) itself (including IP addresses, email addresses, system status data). - Data required for Checkmk to perform the Checkmk OEM Support Services. - Telemetry data such as (but not limited to) a) Checkmk Environment (i) number and types of hosts, services, and folders (this does not include names or paths of folders); (ii) edition and version; b) usage data for checks and plug-ins. The following data is collected per

	plug-in, using the plug-in name as the identifier: (i) number of services created by a plug-in; (ii) number of unique hosts in which a plug-in is active; (iii) number of deactivated services created by a plug-in; c) Grafana integration (i) checks whether a site uses the Grafana integration and transmits (if active); (ii) Grafana version; (iii) whether Grafana is being used; d) configurations of rule sets; e) interactions with the user admin panel; f) number and type of notifications sent; and g) frequency of logins. - The Customer may submit additional Personal Data to Checkmk Cloud (SaaS) and/ or in the context of Checkmk OEM Support, the extent of which is determined and controlled by the Customer at its sole discretion.
Sensitive data processed (if any) and any restrictions or safeguards applied that are appropriate to the nature of the data and the risks associated with it, such as strict purpose limitation, access restrictions (including access only for employees who have received special training), records of access to the data, restrictions on further transfers or additional security measures	The Provider aims for a protection level for the parties concerned by data processing appropriate to the nature and extent of the risk for rights and liberties. **Checkmk Cloud (SaaS) and Checkmk OEM Support for Checkmk Cloud (SaaS) or Checkmk Software (Self-Hosted)** The Provider applies the principle of least privilege for all internal access requirements, with a focus on restricting access to the Checkmk Cloud (SaaS) system environment. Access to all Provider systems is automatically logged within their respective environments, and the log data is transmitted to a designated account accessible only by auditors and security engineers. Customer logs are kept separate from the Provider’s application logs within the region, where they are only accessible with the Customer's consent during an investigation. The same applies to the support systems used in connection with Checkmk OEM Support, as soon as these support systems are provided by the Processor in a cloud environment. - Conduct of video conferences. Live Support in connection with Premium Support is provided exclusively via remote screen sharing during video conferences. Live Support is limited to screen sharing for the sole purpose of real-time assistance and troubleshooting. The Provider is prohibited from taking control of the Customer's IT systems. It is the Customer's sole responsibility to ensure that no personal data of the Customer and/or third parties is visible during Live Support.
Frequency of transmission (e.g., whether transmission is one-time or ongoing)	**Checkmk Cloud (SaaS) and Checkmk OEM Support for Checkmk Cloud (SaaS) or Checkmk Software (Self-Hosted)** - Master data is collected once for the authentication and authorization of the Customer

	and relevant End Users. - Client log files and application log files are transmitted on an ongoing basis for each user session.
Purpose(s) of the processing	**Checkmk Cloud (SaaS) and Checkmk OEM Support for Checkmk Cloud (SaaS) or Checkmk Software (Self-Hosted)** **-** To enable the Provider to perform services for the Customer based on the Subscription Agreement as of the Effective Date regarding the provision of Checkmk Cloud (SaaS) and the provision of Checkmk OEM Support, and to exercise its rights and obligations under the Subscription Agreement. - To enable the Provider to collect and analyze Service-generated Data, in particular Telemetry Data, for the purpose of performance analysis and improvement of Checkmk Cloud (SaaS) and Checkmk Software (Self-Hosted).
Duration for which the Personal Data will be stored or, if this is not possible, the criteria for determining this duration	The Provider stores Personal Data for the duration of the term of the Subscription Agreement regarding the provision of Checkmk Cloud (SaaS) and Checkmk OEM Support Services and for as long as needed for the respective purpose.