DATA PROTECTION AGREEMENT (JOB PROCESSING) Paessler PRTG Hosted Monitoring between the Customer ("Client") and Paessler AG, Thurn-und-Taxis-Straße 14, 90411 Nuremberg/Germany ("Paessler")

1. Object and duration of contract; legal framework

The Client instructs Paessler with processing individual-related data for delivery of PRTG network monitoring services. The duration of this agreement corresponds to the PRTG operation life. This data protection agreement shall be part of the contractual regimes of Paessler PRTG Hosted Monitoring.

2. Nature of data; parties concerned

Paessler processes monitoring data of the Client. Such are PRTG-created personally identifiable data of the Client's applied devices and sensors including data of scope, duration and time of network traffic, data of device identification including IP address and device ID, data of Client accounts using the network as well as data of utilisation of the PRTG account. The Client determines to what extend such monitoring data shall be personalised by selection of applied devices and sensors.
The processing of monitoring data affects users of the devices and network components applied and created by the Client.

3. Rights and responsibilities of client

Assessing the legitimacy of data processing in accordance with article 6 section 1 of GDPR (General Data Protection Regulation) as well as safeguarding the rights of any party concerned in accordance with article 12 to 22 of GDPR shall be the responsibility of the Client.

4. Scope, type, purpose of data processing and directives

(1) The following provisions are final directives regarding the monitoring transferred.

(2) The monitoring data are processed by Paessler solely for the purpose of performing, processing and supporting the PRTG service. This includes the technical provision of the PRTG components, ensuring trouble-free operation, monitoring security risks and system stability, detecting possible problems of the Client's network instance and taking measures to avert the detected problems.

(3) In pursuance of the purpose, Paessler is authorised to read and evaluate the data. Paessler is allowed to log into running PRTG entities in order to analyse existing problems. A user-referred evaluation shall take place if certain user behaviour has been acknowledged as cause for malfunction. Paessler shall inform merely the Client if a certain user or user behaviour has been detected as cause for any problems.

(4) Processing of monitoring data for other purposes, especially the transfer to third parties for other purposes than the agreed purpose, is not allowed. Furthermore, mandated processing shall not include any provision of information to third parties or users of devices and network components applied by the Client. In particular cases, this shall require separate commission.

(5) Paessler may fully anonymize the monitoring data and extract the data that can then no longer be attributed to a person or the Client and use it for the further development and improvement of its products.

(6) Copies or duplicates of the monitoring data shall not be created without prior knowledge of the Client. This does not include backup copies that are required for ensuring smoothly running operation (backup mechanisms and restoring mechanisms) or guaranteeing proper data processing or compliance with any legal archiving duties.

(7) Under normal circumstances, the server shall be operated in an EU member state. Should there exist several location options, the Client shall determine the server location's region upon commission.

5. Technical and organisational protective measures

(1) Paessler shall guarantee a protection level for the parties concerned by data processing appropriate to the nature and extent of the risk for rights and liberties.

(2) This shall include taking technical and organisational measures in accordance with article 32 GDPR to ensure the protection goals of confidentiality, integrity, availability and resilience of the systems and services as well as purpose limitation (prevention of misuse and transfer of monitoring data). The measures taken must be suitable and appropriate to contain risks to these protection goals in the long term and must correspond to the state of the art. The measures to be taken are described/documented.

(3) The measures are subject to technical progress and developments. Alternative measures may be implemented if the protective level of the measures defined is not being undercut.

6. Specific responsibilities of Paessler

(1) Paessler shall process the monitoring data in conformance with the Client's instructions unless Paessler is bound by EU law or law of a member state to process data otherwise (for instance due to investigations by prosecution offices or state security); should this occasion arise, Paessler shall inform the Client of these legal requirements before data procession unless the law in question prohibits such notification for important public reasons (article 28 section 3 sentence 2 letter a of GDPR).

(2) All Paessler employees responsible for order completion are subject to an obligation of confidentiality or obligation of silence. They were made familiar with the relevant rules concerning confidentiality, especially given the subject matter of this agreement.

(3) Paessler shall regularly check the rules laid down in this agreement, especially regarding implementation and – if necessary – amendment of protective measures in order to guarantee that data processing within their area of responsibility follows the requirements of the valid data protection legislation and assure protection of the entities concerned. Paessler may prove adoption of sufficient protective measures by presenting certificates.

7. Subcontracting relationships

(1) The Client shall agree to involvement of subcontractors for processing of the monitoring data on condition that these subcontractors are bound by this agreement and capable of meeting the agreed requirements to the processing of data. The subcontractors involved are listed in annex 1.

(2) Paessler shall inform the Client of all changes regarding involved subcontractors. Should the Client not consent to a subcontractor, they may cancel the PRTG service by exceptional right of termination and end any processing of monitoring data.

8. Violations of protection and reporting obligation

(1) Paessler is obliged to notify security breaches in their range of control and organisation affecting personal data provided by the Client promptly to the Client (article 4 point 12 GDPR). For this purpose, Paessler shall notify the Client immediately of the

respective event through the email address listed and stored in the contact data.

(2) Paessler – in consultation with the Client – shall take appropriate measures to safeguard monitoring data and also take provisional measures to mitigate possible negative effects.

(3) The Client is responsible for reporting that is possibly resulting from article 33 section 1 and article 34 GDPR.

9. Deletion of data

(1) The monitoring data shall be stored for 12 months and overwritten afterwards.

(2) After termination of the PRTG service, the monitoring data shall be deleted six months after the contractual end at the latest. A dispute between the parties regarding contractual services or unresolved claims may result in monitoring data being withheld for evidentiary purposes.

10. Rights of parties concerned

(1) In so far as their means allow, Paessler shall support the Client with their obligations to implement the rights of data subjects.

(2) At the request of the Client, Paessler shall delete the monitoring data involved in data processing. Furthermore, Paessler may correct or delete data or restrict data processing (block) merely upon documented instruction by the Client.

(3) If a data subject contacts Paessler directly regarding their rights (for instance information, correction or deletion of their data), Paessler shall transmit this request to the Client without delay.

11. Obligation to secrecy

The parties commit to treating all information regarding protective measures of the other party and received within the contractual relationship confidentially as trade and business secrets. This obligation to secrecy shall continue even after the end of the contractual relationship.

12. Formal requirements; severability clause

(1) Amendments or supplements to this agreement shall be binding only if made in writing.

(2) If a determination of this agreement should be ineffective or become ineffective, this shall not affect the overall effectiveness of this agreement.

The contractual parties shall endeavour to replace the invalid or unenforceable provision by a valid and enforceable provision.

Annex 1: Subcontractors

Status as of November 25, 2020.

Paessler shall integrate the following subcontractors into the processing of monitoring data:

Enterprise	**Full Address**	**Service**
Amazon Web Services Inc.	410 Terry Avenue North Seattle WA 98109, USA	Hosting of Client entities as well as the Client portal my-prtg.com
SendGrid Inc.	1801 California Street, Suite 500 Denver, Colorado 80202, USA	E-mail transmission for operating my-prtg.com
Slack Inc.	500 Howard St, San Francisco, CA 94105, USA	Messaging and troubleshooting

Annex 2: Preventive Measures

Status as of November 25, 2020.

Measures shall be put into effect to eliminate high and increased risks.

a) Risk model:
When it comes to the assessment of risks, the following model shall form the basis.

Very low risk	Probability of occurrence is practically out of the question, low or very low potential for damage
Low risk	Low probability of occurrence, low potential for damage
Medium risk	Potential probability of occurrence, medium or low potential for damage
Increased risk	Occurrence is to be expected at a medium or low potential for damage or - potential probability of occurrence at a high potential of damage
High risk	Occurrence is to be highly expected, high potential for damage

b) Actions:

Risk fields	**Protective measures regarding monitoring data**
Breach of confidentiality	
• External attacks	- *Process for fast security updates to minimize the attack surface* - *White list of allowed ports/interfaces and firewall rules to minimize the attack area* - *Encrypted network communication (TLS) to prevent the data from being read along* - *Audit logs for all accesses to accounts are generated and checked* - *Isolation of individual customer instances in "virtual data centers" (separated networks and servers) in order to prevent the intrusion from compromised instances.* - *Operation in a certified data center in order to maintain the associated basic security* -
• Unauthorised access, unauthorised login	- *Two-factor authentication of Paessler employees for special protection of administrator accounts* - *Access only after authentication and authorization* - *Encrypted storage of passwords (SHA, salted) to prevent readout* - *Logged employee access for proactive troubleshooting due to internal monitoring measures* - *Logged employee access to troubleshoot errors reported by customer*
• Unauthorised intrusions	- *Logging of the access with evaluation procedures* - *Isolation of individual customer instances in "virtual data centers" (separated networks and servers) in order to prevent the intrusion from compromised instances* - *Operation in a certified data center in order to maintain the associated basic security*
• Unsafe data transfer	- *Encrypted network communication (TLS) to prevent the data from being read along* - *Signed certificates for a validable identity of the servers*
Violation of integrity	
• Unauthorised alteration of data by external attack	- *Logging of data changes with time stamp* - *Minimization of damage through regular backup and restore mechanisms* - *Operation in a certified data center in order to maintain the associated basic security*
• Unauthorised alteration of data by internal attack	- *Logging of data changes with time stamp* - *Minimization of damage through regular backup and restore mechanisms*
• Technical failure	- *Redundant storage (SAN) with checksums* - *Minimization of damage through regular backup and restore mechanisms* - *Isolation of individual customer instances in "virtual data centers" (separated networks and servers) to prevent data from being changed across instance boundaries* - *Operation in a certified data center in order to maintain the associated basic security*
Violation of availability	
• External attacks	- *Isolation of individual customer instances in "virtual data centers" (separated networks and servers) in order to limit failures to individual instances* - *Operation in a certified data center in order to maintain the associated basic security* - *Operation with CDN to absorb peak loads (especially DoS attacks)*
• Technical failure	- *Operation of the customer instances in different data centers, in order to intercept the failure of an entire data center* - *Redundant storage (SAN) with checksums* - *Minimization of damage through regular backup and restore mechanisms* - *Operation in a certified data center in order to maintain the associated basic security* - *Operation with CDN to bridge short-term failures*