Thomas-Krenn.AG's Specific Terms and Conditions for Cloud Services

Version: May 2, 2024

§ 1 Scope

(1) These Specific Terms and Conditions for Cloud Services (hereinafter referred to as "**Cloud STCs**") apply to all contractual relationships between Thomas-Krenn.AG and the Customer regarding the subject matter of the contract specified in Sec. 2.

(2) These Cloud STCs apply in addition to the General Terms and Conditions ("**GTCs**") of Thomas-Krenn.AG (see Sec. 1 (2) of the GTCs, available at: https://www.thomas-krenn.com/de/unternehmen/impressum/agb.html) and shall take precedence over them if provisions in the contractual documents contradict each other in whole or in part.

(3) Within an ongoing contractual relationship, these Cloud STCs also apply to all future contracts to be concluded for the ordering and use of services in accordance with Sec. 2, even if Thomas-Krenn.AG does not refer to them again when the contract is concluded, unless expressly agreed otherwise between the Contractual Parties.

§ 2 Subject matter of the contract

(1) Thomas-Krenn.AG provides services to the Customer in the area of Cloud Computing and the cloud service model Infrastructure as a Service ("**IaaS**"), in particular the operation and provision of virtual IT infrastructure components (especially processor performance, memory, storage space/storage, network resources) in data centers of Thomas-Krenn.AG and/or other contract processors in the form of the public cloud for use by the Customer on a temporary basis (rental) with flexible usage and billing models ("pay per use", "as a service") (hereinafter referred to as "**IaaS services**"; the virtual IT infrastructure environment provided to a customer on an IaaS basis is hereinafter also referred to as "**IaaS environment**"), as well as associated additional services (e.g. Kubernetes, managed services, provision of third-party software; hereinafter collectively referred to as "**services**").

(2) IaaS environments are generally made available to the Customer in the form of the public cloud on demand and generally in real time. A "**public cloud**" can be used by the general public and is therefore open to an indefinite number of users for shared use. Thomas-Krenn.AG only provides services from a "**private cloud**", which is available to the Customer for exclusive use, on the basis of an express separate agreement.

(3) The specific technical configuration of an IaaS environment as well as its scope, the location(s) of the underlying data centers, certifications and further details of the services agreed between the Contractual Parties result from the ordering of services via the website of Thomas-Krenn.AG at www.thomas-krenn.com (hereinafter "**website**") or from another agreement, the respective service descriptions and attachments as well as from any expansion or reduction of services (hereinafter "**scaling**"), which the Customer can carry out themselves at any time by means of so-called "self-provisioning" via an administration interface available in their customer account (hereinafter "**account**") as an interface for controlling the resources of their IaaS environment. Any scaling and other changes to services made by the Customer in their account shall constitute a binding contractual offer or a binding offer to amend the contract; Sec. 3 (3) shall apply accordingly.

(4) The monthly availability of the IaaS environment is the subject of the Service Level Agreement (SLA) agreed in **Annex 1**.

(5) In the event of contradictions between details of an order and/or scaling and/or another agreement, annexes referred to or between different annexes and these GTCs, the following list shall determine the order of precedence:

- The details from service orders made via the website or scaling details specified via the account, other direct agreements between the Contractual Parties
- Service descriptions
- The Service Level Agreement (SLA) in accordance with **Annex 1**
- The agreement on order processing pursuant to Art. 28 GDPR (**Annex 2**) and its annexes
- These Cloud STCs
- The GTCs of Thomas-Krenn.AG

(6) The IaaS environment is connected to the internet ("**upstream**") via Thomas-Krenn.AG's own data network operated at the respective data center location as well as the data networks of third parties (so-called carriers) and network nodes (e.g. DE-CIX) connected to it. The service provided by Thomas-Krenn.AG is limited solely to data communication between the IaaS environment and the data networks of third parties or network nodes. Thomas-Krenn.AG has no influence on data traffic and data packet runtimes outside its own data network and is therefore not responsible for the successful forwarding of data packets from or to an IT system requesting them. The Customer has no claim to the use of certain third-party data networks and network nodes. Thomas-Krenn.AG is entitled to change its own data network as well as the data networks of third parties and network nodes connected to it at any time, provided that basic accessibility of the IaaS environment via the internet is guaranteed. Any information about Thomas-Krenn.AG's own data network and the data networks of third parties and network nodes connected to it (e.g. on the Thomas-Krenn.AG website or in service descriptions) serves only to inform the Customer about the current status of the network.

(7) The Customer does not acquire ownership or expectant rights to the IaaS environment, nor does it have any claims to the surrender of the storage media on which an IaaS environment is based due to the fact that Customer data is stored there.

§ 3 Registration and creation of an account, acceptance of contract

(1) The use of an IaaS environment and its temporary provision (rental) generally requires the Customer to register by creating an account on the website in accordance with Sec. 3 (1) of the GTCs. However, when using the IaaS environment, the account can initially be used as a **trial account** for a certain period of time specified on the website in order to test services free of charge. To order specific services, the customer must convert the trial account into a **paid account**. To do this, payment details, usually a bank account or credit card, must be entered and saved in the account.

(2) The data and prices for the scope of services ordered by the Customer are stored by Thomas-Krenn.AG. They can be called up in the account at any time. The scope of services can also be adjusted by the Customer at any time via scaling (see Sec. 2 (3)).

(3) Thomas-Krenn.AG is entitled to review the Customer's binding contract offer and either accept or reject it within 7 working days of receipt (informing the Customer in the event of cancellation). The Customer is bound to their contractual offer during this review. Acceptance of the Customer's

contractual offer takes place with a separate order confirmation (in text form) or implicitly with the provision of the services, in particular the access data for the IaaS environment provided by Thomas-Krenn.AG.

§ 4 Duties and obligations of the customer, data backups

(1) The Customer is responsible for the selection services and their suitability for the specific intended purposes, unless Thomas-Krenn.AG has expressly advised the Customer in this regard.

(2) The Customer must notify Thomas-Krenn.AG of any defects and errors in the IaaS environment immediately upon discovery in text form and in a comprehensible manner.

(3) The Customer shall keep their details in the account up to date and complete. If the Customer's personal details change, the Customer is responsible for updating them. The Customer can make all changes themselves at any time in the account under "Login".

(4) The passing on of passwords for access to the account and services of Thomas-Krenn.AG is prohibited. The Customer is obliged to keep passwords secret and not to disclose them to third parties, i.e. persons outside their company or persons in their company who are not authorized to represent them, and make them inaccessible to such persons. If the Customer suspects that their account access has been compromised, they must inform Thomas-Krenn.AG immediately and change the password or have it changed by Thomas-Krenn.AG. Otherwise, Thomas-Krenn.AG will relate every activity that takes place via a customer account to the registered customer, with the consequence that the Customer is liable for services used and activities carried out by unauthorized third parties via their account and must, for example, pay IaaS usage fees or compensate for damages incurred.

(5) The Customer must comply with the applicable legal provisions when using the services. In particular, it may not infringe any third-party rights, such as intellectual property rights or personal rights.

(6) The Customer shall ensure that no domains are used on the IaaS environment and that no content is stored that violates laws, official requirements or third-party rights. Furthermore, no content protected by copyright may be illegally distributed via the IaaS environment. In addition, the Customer may not use the IaaS environment for illegal activities or activities that impair IT infrastructure or network components as well as the general IT security at a data center location of Thomas-Krenn.AG or another commissioned processor (e.g. applications, scripts and other techniques that particularly overload IT infrastructure and network components and/or have a negative impact on IaaS environments of other customers). The IaaS environment must also not be used as a platform for hacking attacks or DDoS attacks. In such cases, as well as in the event of the assertion of claims by third parties that are not obviously unfounded, Thomas-Krenn.AG is entitled to block the network connection of the affected IaaS environment in whole or in part until the Customer has eliminated the impairment. In the event of a significant breach of the aforementioned obligations, a particular urgency, imminent danger, an official/judicial order or a legal obligation, Thomas-Krenn.AG may block the connection to the IaaS environment without setting a reasonable deadline or other prior notice, but may inform the Customer of this blocking immediately.

(7) If claims are asserted against Thomas-Krenn.AG by third parties due to possible legal infringements caused by the Customer's use of Thomas-Krenn.AG's services, the Customer shall provide Thomas-Krenn.AG with the necessary support in its legal defense and indemnify Thomas-Krenn.AG against the claims asserted and the costs of legal defense. The prerequisite for this is that Thomas-Krenn.AG informs the Customer immediately of any claims asserted, does not make any concessions or

acknowledgements or declarations with the same or similar effect and enables the Customer to conduct all judicial and extrajudicial negotiations regarding the asserted claims at its own expense.

(8) Unless expressly agreed between the Contractual Parties, Thomas-Krenn.AG does not provide any data backup services. The creation of backup copies is the responsibility of the Customer. For the purpose of protection against possible data loss, the Customer must back up all data and programs that may not be stored in the data center of Thomas-Krenn.AG at regular intervals on its own responsibility and thereby ensure that lost data can be restored with reasonable effort. The scope and frequency of the data backup shall be determined by the Customer, taking into account the value of the data and its importance for its business operations.

§ 5 Modification of services, adaptation to the state of the art

All services are constantly updated, improved and adapted to the advancing state of the art. Thomas-Krenn.AG is therefore entitled to change services at its reasonable discretion, even during the term of the contract, provided that this does not impair the functionality or security function of the services and the Customer does not have to make more than insignificant subsequent investments in order to continue using the services.

§ 6 Rights of use, copyright

(1) Thomas-Krenn.AG grants the Customer a simple, non-exclusive right to use the services for the duration of the contract and limited to the scope of services, which is otherwise unrestricted in terms of territory and subject matter. The right of use includes use within the scope of business operations. The right of use does not include the right to edit the services or the right to grant sublicenses. Any further transfer of the services to third parties by way of reselling requires a separate agreement between the Contractual Parties.

(2) Thomas-Krenn.AG reserves the right of ownership or copyright to all offers and cost estimates submitted by it as well as illustrations, calculations and other documents made available to the Customer. The Customer may not make these accessible to third parties, disclose them, use them or reproduce them – whether themselves or through third parties – without the express consent of Thomas-Krenn.AG. At the request of Thomas-Krenn.AG, the Customer must return these items in full to Thomas-Krenn.AG and destroy any copies made if they are no longer required by the Customer in the ordinary course of business or if negotiations do not lead to the conclusion of a contract. This does not apply to the storage of electronically provided data for the purpose of standard data backups.

§ 7 Prices, payment, due date, invoicing, blocking in the event of late payment

(1) The Customer is obliged to pay the invoice amounts in accordance with the prices agreed.

(2) Additional or special services shall be invoiced separately. If no price has been agreed for services or for additional or special services, these services shall be charged according to the current price information on the website. Thomas-Krenn.AG is entitled to change the prices on the website at any time.

(3) In the case of a usage-based fee, Thomas-Krenn.AG is also entitled to issue a separate invoice within one month if the current fee claim exceeds the usual invoice amount of the previous months by 50% or more and/or a threshold amount agreed with the Customer or, unless otherwise agreed, an invoice amount of EUR 500.

(4) Unless otherwise agreed, invoices shall be issued in electronic form by making the invoice available for retrieval in the account and, on request, to the e-mail address provided by the Customer. The Customer expressly agrees that invoices will not be sent via postal services.

(5) If the Customer is in arrears with the payment of the monthly basic fee for two consecutive payment dates or is in arrears with the payment of an amount equal to the monthly basic fee for two months in a period that extends over more than two payment dates, Thomas-Krenn.AG is free to block the Customer's IaaS environment for access via the internet without setting a deadline and further notice. The temporary blocking of services does not affect the Customer's obligation to pay.

§ 8 Term of the contract, termination

(1) Unless otherwise agreed, a contract for the provision and use of an IaaS environment is concluded for an indefinite period of time (rental). The parties may also agree a minimum contract term.

(2) Each contractual party may terminate the contractual relationship as a whole or individual contractual components or contracts at any time by giving 4 weeks' notice to the end of the month.

(3) The Customer's right to terminate the contract at any time in accordance with Sec. 648 sentence 1 BGB, insofar as the law on contracts for work and services is applicable, is excluded.

(4) The right to terminate the contract without notice for good cause remains unaffected. An valid reason exists for Thomas-Krenn.AG in particular if the Customer:

a) Is in arrears with the payment of the monthly basic fee for the use of the services for two consecutive payment dates

b) Is in arrears with payment of an amount equal to the basic monthly fee for two months in a period extending over more than two payment dates

c) Culpably breaches a material contractual obligation and fails to remedy the situation within a reasonable period of time despite a warning

d) Seriously or repeatedly breaches its obligations under Sec. 4 (6) or other obligations under the contract that protect IT security or the rights of third parties

e) Violates statutory prohibitions, in particular copyright, trademark, name, data protection or competition law provisions, insofar as this impairs material rights or interests of Thomas-Krenn.AG in more than an insignificant manner.

(5) Any termination must be in writing to be effective. If Thomas-Krenn.AG provides the Customer with corresponding termination options for IaaS services in their account, the contract can also be effectively terminated via this option.

(6) Irrespective of the possibility of termination, the Customer has the option of reducing individual services in their account by means of scaling and thereby bringing about a change to the contract (see Sec. 2 (3)).

(7) Upon termination of the contract – for whatever legal reason – all rights of use granted to the Customer within the scope of the provision of services shall lapse. Thomas-Krenn.AG will delete all data and settings at the end of the contract.

§ 9 Indemnification, rights of third parties

(1) The Customer is obligated to indemnify Thomas-Krenn.AG internally against all possible claims by third parties that are based on illegal or infringing actions by the Customer or errors in the content of the information provided by the Customer. This applies in particular to copyright, trademark, name, data protection and competition law violations as well as violations of Sec. 4 (6).

(2) If a third party justifiably asserts claims against the Customer due to the infringement of an industrial property right or copyright owing to the use of the services of Thomas-Krenn.AG in the Federal Republic of Germany and the Customer is thereby impaired in the use of the services of Thomas-Krenn.AG or prevented from using them, the following provisions pursuant to Sec. 9 (3) to (5) shall apply.

(3) Thomas-Krenn.AG shall, at its discretion and expense, either modify or replace the services owed in such a way that the asserted industrial property right or copyright is no longer infringed, but essentially corresponds to the service owed in a manner that is reasonable for the Customer, or indemnify the Customer from license fees vis-à-vis the third party. The prerequisite is that the Customer informs Thomas-Krenn.AG immediately of the assertion of the claims, does not acknowledge the alleged infringement of property rights and leaves any disputes with the third party, including any out-of-court agreements, to Thomas-Krenn.AG or only conducts or undertakes them in agreement with Thomas-Krenn.AG. If the Customer ceases to use the services of Thomas-Krenn.AG in order to minimize damages or for other important reasons, the Customer is obliged to inform the third party that the cessation of use does not constitute an acknowledgment of the alleged infringement of property rights.

(4) Insofar as the Customer is responsible for the asserted infringement of property rights, for example because it has modified or processed the services of Thomas-Krenn.AG without authorization, or has used the services of Thomas-Krenn.AG in an unauthorized manner, claims by the Customer against Thomas-Krenn.AG under this Sec. 9 are excluded.

§ 10 Warranty

(1) Thomas-Krenn.AG points out to the Customer that it is currently not possible to provide and operate an IaaS environment for the Customer in such a way that it functions without crashes or errors in all application combinations or can be completely protected against manipulation by third parties. Furthermore, Thomas-Krenn.AG does not guarantee that a provided IaaS environment meets the specific requirements of the Customer, in particular that it is suitable for certain applications and is free of malware.

(2) If the contractual use of services is suspended as a result of a defect that is subject to the liability for defects under the rental agreement, the Customer shall be released from payment of the remuneration for the impaired service for the period in which use is suspended. For the period during which the suitability for contractual operation is reduced, the Customer shall only have to pay a reasonably reduced fee. Insofar as separate service levels have been agreed between the Contractual Parties for the service affected by a defect and these provide for a reduction in the remuneration, the provisions of the Service Level Agreement (Annex 1) shall apply conclusively to the reduction and any exclusion of the remuneration obligation.

(3) Insofar as Thomas-Krenn.AG's services are subject to liability for defects under the contract for work and services, Thomas-Krenn.AG has the right to choose whether to provide subsequent performance. If Thomas-Krenn.AG is not in a position to rectify the defect or provide a fault-free replacement, Thomas-Krenn.AG will provide the Customer with workarounds. Insofar as these are reasonable for the Customer, they shall be deemed subsequent performance. The warranty period is one year from delivery/performance or, if acceptance is required, from acceptance. This period does not apply to Customer claims for damages arising from injury to life, limb or health or from intentional or grossly negligent breaches of duty by Thomas-Krenn.AG or its agents, which expire in accordance with the statutory provisions.

(4) In all other respects, customers are entitled to the statutory rights in the event of defects.

§ 11 Liability for damages

(1) Thomas-Krenn.AG's liability for damages is governed by Sec. 11 of the GTCs. In addition, the following paragraphs 2 and 3 apply.

(2) Thomas-Krenn.AG uses TSL/SSL encryption for certain security-relevant data transmissions and connections. Despite the current state of technology, data communication via the internet cannot be guaranteed to be error-free and/or available at all times. Liability for constant and uninterrupted availability is therefore excluded unless there is a separate contractual agreement with the Customer.

(3) In the event of a loss of data stemming from simple negligence on the part of Thomas-Krenn.AG, the company is exclusively liable for the damages that would have occurred even if the Customer performed a standard backup of the data in accordance with Sec. 4 (8), particularly for any costs incurred in restoring the data. Thomas-Krenn.AG is not liable for the loss of data and/or programs insofar as the damage is based on the fact that (1) the Customer has failed to carry out proper data backups and thereby ensure that lost data can be restored with reasonable effort or that (2) the Customer has failed to carry out the timely installation and application of patches or updates.

§ 12 Confidentiality

(1) The Contractual Parties are obliged to keep the content of this contract and the information disclosed or obtained by the other contracting party and/or a company affiliated with it within the meaning of Sec. 15 et seq. AktG (German Stock Corporation Act) in connection with this contract orally, in writing or in any other way (hereinafter "**confidential information**") confidential during the term of the contract and also after its termination.

(2) This obligation shall not apply to confidential information which was already known to the receiving party when the contract was concluded, which is publicly known when the contract is concluded or is made public thereafter, which must be disclosed due to legal obligations or by order of a court or authority.

(3) The receiving contracting party also undertakes to use confidential information exclusively for the purposes of implementing this contract and not to disclose it either directly or indirectly to third parties, but only to make it accessible to those employees and consultants who need to know the confidential information for the implementation of this contract and who are obliged to maintain confidentiality accordingly. Companies affiliated with the receiving contracting party within the meaning of Sec. 15 et seq. AktG shall not be deemed to be third parties within the meaning of the preceding sentence, provided that these companies are obliged to maintain confidentiality vis-à-vis the receiving

contracting party and have also obliged their employees and consultants to maintain confidentiality accordingly. All rights to the confidential information shall remain with the respective disclosing contracting party.

§ 13 Data protection

(1) Thomas-Krenn.AG collects, processes and uses the Customer's personal data in accordance with the statutory data protection regulations. Additional information on this can be found in the Privacy Policy on the Thomas-Krenn.AG website.

(2) The Customer is the sole controller within the meaning of the General Data Protection Regulation (GDPR) with regard to personal data that it processes using the services of Thomas-Krenn.AG. In this respect, the Customer must ensure compliance with all data protection regulations.

(3) Insofar as Thomas-Krenn.AG processes personal data when providing its services to the Customer, the Contractual Parties shall conclude the data processing agreement attached as Annex 2 to this contract. Thomas-Krenn.AG will process the relevant personal data solely in accordance with the provisions set out therein and in accordance with the Customer's instructions.

§ 14 Amendment of these terms and conditions

Thomas-Krenn.AG is entitled to unilaterally amend these Cloud STCs insofar as this is necessary to adapt to changes in the legal or technical framework or to eliminate any subsequent equivalence problems. It shall inform the Customer of the amended regulations in text form. The amendment shall become part of the contract unless the Customer objects in writing to its inclusion in the contractual relationship within 4 weeks of receipt of the notification of amendment. In the event of an objection by the Customer, Thomas-Krenn.AG is free to provide the services on the basis of the previous Cloud STCs or to terminate the contract with the Customer in compliance with the ordinary notice period in accordance with Sec. 8 (2).

§ 15 Final provisions

The place of performance for all obligations arising from the contractual relationship shall be the respective data processing locations (data centers on which the IaaS environment is based), unless otherwise specified.

Annex 1

Service Level Agreement (SLA)

§ 1 Subject matter of the contract

(1) This Service Level Agreement ("**Service Level Agreement**" or "**SLA**" for short) regulates and defines performance parameters ("**Service Level**") for the provision of services in connection with the provision of an IaaS environment by Thomas-Krenn.AG as well as the determination of credits and other measures as a result of non-compliance.

(2) Should provisions in the Cloud STCs or the GTCs of Thomas-Krenn.AG contradict provisions of this SLA in whole or in part, the provision in this SLA shall take precedence.

§ 2 Scope of application

This SLA shall not apply as long as the Customer is in default of payment and in all cases attributable to:

- Legal/regulatory requirements or court orders
- Changes to a service or configuration that has been performed or commissioned by the Customer
- Blocking of individual services or an entire account due to improper use by the Customer

§ 3 Services of the IaaS environment

(1) The IaaS environment provided to the Customer by Thomas-Krenn.AG at one or more locations consists of controlling, primary and secondary services. All services of the IaaS environment not mentioned under (1) and (2) below are secondary services.

a) Controlling services

(i) The **API** is an interface operated by Thomas-Krenn.AG that allows the Customer to configure all services. The API is based on a standardized RESTful-HTTP interface.

(ii) **API CLI** is a command line interface provided by Thomas-Krenn.AG that allows the API of Thomas-Krenn.AG to be operated.

(iii) **API GUI** is a web interface provided and hosted by Thomas-Krenn.AG that allows the API of Thomas-Krenn.AG to be operated.

(iv) **Automation Services** are services operated by Thomas-Krenn.AG that perform certain activities in an automated manner based on criteria defined by the Customer. For example, snapshots of individual virtual hard drives can be created and archived automatically, or additional CPU resources can be provided automatically in the event of certain workload parameters (e.g. CPU utilization on a virtual server).

b) Primary services

(i) **Compute and computing resources** are the resources of the IaaS environment that form a virtual server, in particular processor cores (CPU), memory (RAM), network interface cards (NIC) and primary block storage (storage).

(ii) **Upstream** is the connection between the IaaS environment and the internet.

(iii) **Private network** is the connection between the Customer's virtual servers via a software-defined network (SDN).

(2) Thomas-Krenn.AG also provides an interface at one or more locations that allows the Customer to request high-quality IT services and programs (managed Platform-as-a-Service (**PaaS**) services, e.g. S3 storage, load balance, firewall, message gateway, databases, Kubernetes orchestration, etc.).

§ 4 Availability, maintenance work, monitoring

(1) Thomas-Krenn.AG guarantees the availability specified in the following table ("**availability**") in the calendar month with regard to the services specified in Sec. 3. A calendar month refers to a month with a calculated 30.5 days, regardless of the actual number of calendar days.

Service	Availability	Criterion	Examples
Primary service	99.99%	Interruption of a primary service	**SLA violated:** Upstream is unreachable from at least two different regions of the world for two consecutive measuring points. **SLA not violated:** A CPU system freezes unannounced. The monitoring sensor correctly detects this condition within a tolerance of 120 seconds and performs an autorecovery procedure according to the Customer's settings.

Controlling service	99.99%	Inaccessibility of API interfaces or non-execution of API commands or automation services not executed on time.	**SLA violated:** Out of 10,000 requests from the Customer to Thomas-Krenn.AG's API, more than one error occurs. **SLA not violated:** For every 100,000 API requests, there is one failed API request
PaaS	99.99%	Interruption of the operation or accessibility of the respective PaaS service.	**SLA violated:** A load balancer service is not available for more than 264 seconds in the respective billing month or the function is disrupted. **SLA violated:** A PaaS database cluster does not respond to queries for more than 264 seconds in a given month.
Secondary	99.9%	Secondary services are not available or generate a non-operational error.	A secondary service is not available for more than 44 minutes in a given month.

(2) The services referred to in paragraph 1 are available if they have been provided or are available in the agreed period in accordance with the percentage availability rate agreed in paragraph 1. The availability rate is calculated as follows:

$$\frac{\text{(Agreed availability time – Unplanned downtime)}}{\text{Agreed availability time}}$$

(3) The period during which Thomas-Krenn.AG must provide the services owed is 24 hours a day, seven days a week (hereinafter "**agreed availability time**").

(4) The period from the occurrence of the unavailability of the services within the agreed availability period until the end of the unavailability is defined as **unplanned downtime**. When determining the availability or the availability rate, the following downtimes are not taken into account:

a) Those for which Thomas-Krenn.AG is not responsible, in particular impairments that are based on failures and/or malfunctions of IT systems or other technical systems and/or network components outside the area of responsibility contractually assumed by Thomas-Krenn.AG; in particular:

- Outages caused by incoming attacks (e.g. DDoS attacks)
- Outages for which Thomas-Krenn.AG is not directly responsible (such as external DNS server problems, failures of parts of the internet outside the control and operating services of Thomas-Krenn.AG)
- Outages caused by force majeure
- Outages caused by the Customer due to overloading and/or incorrect or improper use/operation of the services provided by Thomas-Krenn.AG

- Outages caused by failure to cooperate on the part of the Customer or third parties commissioned by the Customer

b) Planned maintenance work carried out as agreed in accordance with paragraph 5 below or maintenance work otherwise agreed with the Customer

c) Unforeseen required maintenance work for which Thomas-Krenn.AG is not responsible

d) Unforeseen events (e.g. critical security patches that require unannounced maintenance)

(5) As agreed, Thomas-Krenn.AG carries out scheduled maintenance work (e.g. for non-critical updates) usually between 10:00 pm and 6:00 am. Thomas-Krenn.AG generally operates a zero-downtime architecture, which means that the vast majority of updates have no impact on performance. Should maintenance work nevertheless affect or interrupt the Customer's services (e.g. if more than one service component is affected simultaneously), Thomas-Krenn.AG will notify the Customer of such planned maintenance work at least three working days in advance by e-mail.

(6) Notwithstanding paragraph 5 above, maintenance work or force upgrades to platform services (in particular management platforms) shall be announced to the Customer by e-mail and in the notification center of the Partner and Cloud Panel at least 3 weeks before the maintenance. If possible, a time window will be agreed between Thomas-Krenn.AG and the Customer.

(7) Maintenance work on individual components to which only one customer has access (e.g. dedicated hardware) is coordinated with the Customer on a case-by-case basis and, if possible, carried out by mutual agreement at a time that is convenient for the Customer.

(8) Maintenance work may be carried out immediately and without prior notice if events occur that require immediate action (e.g. imminent danger, critical patches, significant impairment of IT security).

(9) The services referred to in paragraph 1 shall be subject to permanent monitoring. A wide range of sensors and monitoring technologies are used to identify malfunctions before they occur (so-called predictive failure detection, **PFD**) and automatically take suitable measures to move services used by the Customer to a zone that is not affected by a malfunction. Further, reactive instruments are used that automatically restore the service used by the Customer when a malfunction occurs and, if necessary, automatically alert Thomas-Krenn.AG's corresponding IT experts and involve them in the fault clearance. To ensure PFD, it is necessary for Thomas-Krenn.AG to collect sensor information and process it automatically (so-called machine learning and profiling). In particular, information regarding customer workloads, the behavior of specific workloads, automated operations using Thomas-Krenn.AG's API, the response behavior of hardware and software, hardware and sensor temperatures, power supply readings and statistically relevant data about the behavior of the platform operated by Thomas-Krenn.AG, including PaaS services, is collected. No personal data within the meaning of the GDPR is collected and processed as part of the PFD.

(10) Thomas-Krenn.AG's upstream is monitored from different regions of the world. In some cases, external service providers are used, which allow Thomas-Krenn.AG's NOC to log a measurement of latencies, packet losses and changes in routing paths. The upstream is considered unavailable once two consecutive checks from at least two different regions of the world have revealed unavailability.

§ 5 Response times

(1) The response time for service disruptions, availability restrictions or availability failures is 30 minutes within business hours and 120 minutes outside business hours (business hours are from 7:00 am to 10:30 pm on working days, with the exception of national and Bavarian public holidays, Christmas Eve and New Year's Eve). Response time is the period of time between the receipt of a qualified fault report from the Customer by telephone, e-mail or ticket and the written confirmation of an existing fault by Thomas-Krenn.AG via e-mail. The response time therefore begins when Thomas-Krenn.AG receives the notification from the Customer. It is complied with if the Customer receives initial information or notifications regarding the possible causes of the malfunction or problem solution within the response time or if Thomas-Krenn.AG makes the first qualified attempt to analyze and rectify the malfunction.

(2) Thomas-Krenn.AG is free to decide at its own discretion which means it will use to remedy a disruption. Thomas-Krenn.AG may, if possible, provide a temporary solution ("work around") until the fault has been completely rectified if the faults cannot be rectified within this period.

§ 6 Reporting a fault, technical support

The Customer is obliged to inform Thomas-Krenn.AG immediately of any recognizable disruptions to the services, availability restrictions or failures to technical support by e-mail or the ticket system. The Customer should describe the problems as precisely as possible. Technical support also provides assistance and advice on troubleshooting. Thomas-Krenn.AG assigns a processing number ("**ticket**") for each customer request.

§ 7 Remuneration

The remuneration for the provision of the services is regulated in the main contract. Compliance with the service level defined in the Service Level Agreement is not remunerated separately.

§ 8 Credit notes

(1) In the event of non-compliance with the agreed monthly availability, the parties agree to a reduction in the monthly remuneration for the services concerned in the month in question, which Thomas-Krenn.AG will grant the Customer in the form of a credit note on the following invoice as follows:

Service level – Availability		Credit based on one month's remuneration
From	to	
99.99%	99.50%	5%
99.50%	99.00%	10%
99.00%	98.00%	20%
98.00%	97.00%	40%
97.00%	96.00%	60%

96.00%	95.00%	80%
Under 95.00%		100%

(2) Only the data automatically collected and analyzed by Thomas-Krenn.AG for each service is decisive for the achievement of the SLA. The Customer is not obliged to give notice. Should any measurements taken by the Customer deviate from the measurements taken by Thomas-Krenn.AG by more than 10% to the Customer's disadvantage, the parties shall carry out a joint analysis of the causes and measurement methods. Thomas-Krenn.AG is free to adjust future measurements accordingly at its own discretion.

(3) In the case of time-based measurements, the credit is composed of the duration of an unavailability rounded up to 5 minutes, multiplied by a factor of 10 on the charges incurred for all services directly affected. In case of violation of an SLA related to activity-based measurements, the credits are calculated from the base price per activity, analogous to the time-based measurement with a factor of 10.

(4) The amount of cumulative credits are capped at the Customer's average monthly invoice amount of the previous three months, and not more than the Customer's total invoice amount incurred in the calendar year.

§ 9 Term

This SLA comes into force at the start of the contract and ends automatically upon termination of the contract for IaaS services with Thomas-Krenn.AG.

§ 10 Final provisions

(1) Should one of the provisions of this SLA or a provision subsequently incorporated into it prove to be invalid in whole or in part, or should the SLA contain a loophole, the remaining contractual provisions shall remain unaffected. It is the express intention of the parties to maintain the validity of the remaining provisions under all circumstances and thus to waive Sec. 139 BGB. The invalid provision shall be replaced or the loophole closed by a legally permissible provision that comes as close as possible to the meaning and purpose of the invalid provision.

(2) Thomas-Krenn.AG is entitled to transfer the rights and obligations based on this SLA to third parties, in particular to subcontractors.

(3) Amendments and additions to this SLA must be made in writing, unless otherwise specified.

Annex 2

Agreement on order processing in accordance with Art. 28 GDPR

between

the **Customer** named
in the order confirmation

– Person responsible –

(hereinafter referred to as the **Client**)

and

Thomas-Krenn.AG
Speltenbach-Steinäcker 1
94078 Freyung

– Order processor –

(hereinafter referred to as the **Contractor**)

§ 1 Scope and duration of the order

(1) The subject of the contract is the provision of IT infrastructure services in the area of Cloud Computing and the cloud service model "Infrastructure as a Service (IaaS)" and other services within the scope agreed between the Contractual Parties by order submitted via the website of Thomas-Krenn.AG or in another agreement (hereinafter **main contract**). In the course of the provision of services by the Contractor, access to personal data of the Client cannot be excluded.

(2) The Client alone is responsible for assessing the permissibility of the collection, processing or use and for safeguarding the rights of the data subjects.

(3) The duration of this order (term) is based on the duration of the provision of services by the Contractor to the Client on the basis of the main contract.

§ 2 Specification of the contract content

(1) The scope, type and purpose of the Contractor's access to the Client's data are determined by the IT services agreed with the Contractor in the main contract and the other annexes contained therein. Access options exist in this context in particular:

- In the provision of virtual IaaS environments
- In the technical administration of the IaaS environment and in the provision of installation, configuration and support services

- Through other support activities and support services

For the purpose of fulfilling the contract, access by the Contractor to the data listed in paragraph 2 below cannot be excluded.

(2) Type of data

The data categories of customers, suppliers, business partners and employees of the Client affected by the commissioned activity are as follows:

- Master and address data
- Contact details
- Employee data
- Contract data
- Protocol data
- Traffic data
- Communication data (e.g. e-mail)

(3) Group of data subjects

(4) The group of persons affected by the handling of data within the scope of this contract includes:

- Customers and potential customers of the Client
- Suppliers/service providers and business partners of the Client
- Employees, trainees

§ 3 Technical and organizational measures

(1) The Contractor shall take all necessary technical and organizational measures within its area of responsibility in accordance with Art. 32 GDPR to protect personal data. The measures selected by the Contractor in this respect are documented in **Attachment 1** "Technical and organizational measures" and form part of this agreement.

(2) The agreed technical and organizational measures are subject to technical progress and further development. In this respect, the Contractor is permitted to implement alternative adequate measures in the future. The safety level of the defined measures must not be undercut. The Contractor must document significant changes.

(3) The Contractor shall enable and support the review of the implementation of the agreed measures before the start of and during processing by the Client and shall inform the Client on request about the technical and organizational measures implemented at a data processing site.

§ 4 Rights of data subjects

(1) The Contractor shall support the Client in its area of responsibility and as far as possible by means of suitable technical and organizational measures in responding to and implementing requests from data subjects with regard to their data protection rights. The Contractor may not access, port, correct, delete or restrict the processing of data processed on behalf of the Client without authorization, but only in accordance with documented instructions from the Client. If a data subject contacts the Contractor directly in this regard, the Contractor shall forward this request to the Client without delay.

(2) If included in the scope of services, the rights to information, rectification, restriction of processing, deletion and data portability shall be ensured directly by the Contractor in accordance with the documented instructions of the Client.

§ 5 Obligations of the Contractor

In addition to compliance with the provisions of this contract, the Contractor must comply with further legal obligations under the GDPR and in this respect guarantees compliance with the following obligations in particular:

a) Written appointment of a data protection officer who performs his or her duties in accordance with Art. 38 and 39 GDPR. Their contact details can be found in the Privacy Policy on the Thomas-Krenn.AG website.

b) Maintaining confidentiality in accordance with Art. 28 (3) sentence 2 b, 29, 32 (4) GDPR. When carrying out the work, the Contractor shall only deploy employees who are bound to confidentiality and who have been familiarized in advance with the relevant provisions on data protection, in particular any existing instruction and purpose limitation. The Contractor and any person subordinate to the Contractor who has legitimate access to personal data may only process this data in accordance with the Client's instructions, including the powers granted in this order, unless they are legally obliged to process it.

c) The Client and the Contractor shall cooperate with the supervisory authority in the performance of their tasks upon request.

d) The Contractor shall regularly monitor the internal processes and the technical and organizational measures to ensure that the processing in its area of responsibility is carried out in accordance with the requirements of the applicable data protection law and that the protection of the rights of the data subject is guaranteed.

e) Verifiability of the technical and organizational measures taken vis-à-vis the Client within the scope of its inspection rights in accordance with Sec. 8 of this contract.

f) The Contractor shall report breaches of personal data protection to the Client in such a way that the Client can comply with its legal obligations, in particular in accordance with Art. 33, 34 GDPR.

g) The Contractor shall support the Client in its area of responsibility and as far as possible within the scope of existing information obligations towards supervisory authorities and data subjects and shall provide it with all relevant information in this context without delay.

h) Insofar as the Client is obliged to carry out a data protection impact assessment, the Contractor shall support it, taking into account the type of processing and the information available to it. The same applies to any existing obligation to consult the competent data protection supervisory authority.

§ 6 Subcontracting relationships

(1) Subcontracting relationships within the meaning of this regulation are those services that are directly related to the provision of the main service. This does not include ancillary services used by the Contractor, e.g. telecommunications services, postal/transport services, cleaning services or security services. Maintenance and testing services shall constitute a subcontracting

relationship if they are provided for IT systems that are provided in connection with a service provided by the Contractor under this contract. However, the Contractor is obliged to make appropriate and legally compliant contractual agreements and to take control measures to ensure the data protection and data security of the Client's data, even in the case of outsourced ancillary services.

(2) The Client agrees in principle that the Contractor may subcontract to carefully selected third-party companies. When awarding subcontracts, the Contractor must observe the requirements of the GDPR and draft the contractual agreement with the subcontractor in such a way that it complies with the data protection requirements between the Contractor and the Client set out in this agreement and the provisions of the GDPR.

(3) The client agrees to the commissioning of the subcontractors currently employed, who are named in the list of subcontractors (Attachment 2). The Contractor shall ensure that an up-to-date list of the subcontractors used at any given time ("Subcontractor list") is always available to the Client for retrieval in the Client's account.

§ 7 International data transfers

(1) Any transfer of personal data to a third country or to an international organization requires the consent of the Client and compliance with the requirements for the transfer of personal data to third countries in accordance with Chapter V of the GDPR.

(2) The provision of the contractually agreed data processing takes place exclusively in a member state of the European Union or in another state party to the Agreement on the European Economic Area.

(3) If the Client instructs the transfer of data to third parties in a third country, the Client is responsible for compliance with Chapter V of the GDPR.

§ 8 The Client's rights to inspection

(1) The Client shall have the right, in consultation with the Contractor, to carry out inspections at the Contractor's premises or to have them carried out by inspectors to be named in individual cases. They shall have the right to satisfy themselves of the Contractor's compliance with this agreement by means of spot checks during normal business hours. The checks must be notified in good time. The Contractor shall provide the Client with the necessary information upon request and provide evidence of the implementation of the technical and organizational measures. Costs incurred by the Contractor as a result of its support activities shall be reimbursed to the Contractor to a reasonable extent.

(2) Proof of the technical and organizational measures for compliance with the special requirements of data protection in general and those relating to the order can be provided by current certificates, reports or report extracts from independent bodies (e.g. auditors, internal audit, data protection officer, IT security department, data protection auditors, quality auditors).

§ 9 Authority of the Client to issue instructions

(1) The Contractor shall process personal data only on the basis of documented instructions from the Client unless it is obliged to do so under the law of the Member State or under Union law. The Client shall confirm verbal instructions without delay (in text form). The Client's initial

instructions are set out in this contract.

(2) The Contractor must inform the Client immediately if it is of the opinion that an instruction violates data protection regulations. The Contractor shall be entitled to suspend the execution of the corresponding instruction until it is confirmed or amended by the Client.

§ 10 Deletion and return of personal data

(1) Copies or duplicates of the data will not be created without the knowledge of the Client. Excluded from this are backup copies, insofar as they are necessary to ensure proper data processing, as well as data required to comply with statutory retention obligations and technically necessary data replications in the context of distributed, cross-location cloud use.

(2) After completion of the contractually agreed work or earlier at the request of the Client – but at the latest upon termination of the service agreement – the Contractor shall hand over to the Client all documents, processing and usage results and data pertaining to the contractual relationship that have come into its possession or, with prior consent, destroy them in accordance with data protection regulations. The same applies to test and scrap material.

Attachment 1 (to Annex 1: AV Contract)

Technical and organizational measures (TOM) within the meaning of Art. 32 GDPR

Thomas-Krenn.AG, Speltenbach-Steinäcker 1, 94078 Freyung (**Contractor**)

Version: May 2, 2024

1. Subject matter and scope

Organizations that collect, process or use personal data themselves or on the behalf of third parties must take the technical and organizational measures necessary to ensure compliance with the provisions of data protection laws. Measures are only necessary if their cost is proportionate to the intended protective purpose. 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, the Contractor shall meet this requirement for the services specified in the main contract at the agreed data processing location (data center) by taking the following technical and organizational measures ("**TOM**").

When selecting the measures, the four protection objectives of Art. 32 (1) b GDPR, namely the confidentiality, integrity, availability and resilience of the systems, were taken into account in order to ensure rapid recovery after a physical or technical incident. All TOMs are regularly reviewed for their effectiveness in accordance with Art. 32 (1) d GDPR.

2. Pseudonymization

Pseudonymization is the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable individual.

The pseudonymization and anonymization of the Client's data is generally not part of the services to be provided by the Contractor unless a separate agreement has been expressly made in the main contract.

3. Encryption

Encryption transforms plain text into a ciphertext using additional information, the so-called "key", which should not be decipherable by persons who do not know the key.

The Contractor ensures the encryption of the data in organizational terms through password guidelines and password assignments and in technical terms through the use of common encryption technologies (especially during storage, "at rest") and the use of virtual private networks (VPN) for remote access.

4. Confidentiality (Art. 32 (1) b GDPR)

Confidentiality refers to the protection of personal data from unauthorized disclosure, in particular through entry, access and separation controls.

4.1 Entry control

The subject of entry control are measures that are suitable for preventing unauthorized persons from gaining physical proximity to data processing systems with which personal data is processed or used. The contractor ensures this via:

Technical measures	Organizational measures
• Site security, in particular fences and other spatial boundaries • Building security, in particular securing data center rooms, building shafts and doors • Alarm systems, security locks, locking systems • Video surveillance	• Visitor registration • Visitor books and logs • Obligation of employees and guests to wear ID cards • Reception staff for identity checks • Careful selection of cleaning and security staff

4.2 System-level access control

The subject of system-level access control are measures that are suitable for preventing unauthorized persons from gaining access to data processing systems. The contractor ensures this via:

Technical measures	Organizational measures
• Secure VPN connections • Drive encryption • Firewalls • Locking of racks • Authentication, passwords • Two-factor authentication	• User rights and key rules • Password rules • Use of trustworthy personnel for the areas of security and cleaning • Assignment of user rights

1.3 Data access control

The subject of data access control are measures that ensure that those authorized to use a data processing system can only access the data subject to their access authorization and that

personal data cannot be read, copied, changed or removed without authorization during processing, use and after storage. The contractor ensures this via:

Technical measures	Organizational measures
• Logging of accesses • Drive encryption • Identification and authentication system • Secure data storage	• Authorization concepts • Password rules • Data protection-compliant destruction of drives by service providers

1.4 Separation control

The subject of separation control is the separate processing of data collected for different purposes. The contractor ensures this via:

Technical measures	Organizational measures
• Encryption of data • Separation of data stored for different purposes	• Client separation • Database rights adapted to the respective data records, authorization concepts

2. Integrity (Art. 32 (1) b GDPR)

Integrity refers to ensuring the correctness (integrity) of data and the correct functioning of systems. When the term integrity is applied to "data", it expresses that the data is complete and unchanged. The Contractor ensures the integrity of the data, in particular by means of transfer and input control.

2.1 Transfer control

The subject of transfer control are measures that ensure that personal data cannot be read, copied, changed or removed without authorization during electronic transmission or during their transport or storage on drives, and that it can be checked and determined to which bodies a transmission of personal data by data transmission devices is intended. The contractor ensures this via:

Technical measures	Organizational measures
• VPN technologies	• Regular review of retrieval and transmission processes • Preparation of a procedure directory

2.2 Input control

The subject of input control is measures to subsequently check and determine whether and by whom personal data has been entered, changed or removed in data processing systems. The contractor ensures this via:

Technical measures	Organizational measures
• Protocols	• Authorization concepts • Access authorizations

3. Availability and resilience (Art. 32 (1) b GDPR)

The availability of services, functions of an IT system, IT applications or IT networks or even information is ensured if users can always use these as intended. Systems are resilient if they are so robust that they can function even under heavy access or heavy utilization. The Contractor ensures the availability and resilience of the data as follows:

Technical measures	Organizational measures
• Air conditioning of the server rooms • Uninterruptible power supply (UPS) • Fire and smoke detectors • Fire extinguishers	• Emergency management

4. Ability to restore availability and access (Art. 32 (1) b GDPR)

The Contractor shall ensure the recoverability of availability and access after security incidents by means of emergency concepts and the performance of penetration tests.

5. Procedures for regular review, assessment and evaluation (Art. 32 (1) d GDPR; Art. 25 (1) GDPR)

The Contractor ensures the regular review of data security measures through measures to implement data protection requirements (Art. 25 (2) GDPR), in particular through data protection-friendly default settings (data privacy by design and by default), such as restricting the storage period or access to data, as well as measures that ensure that personal data can only be processed in accordance with the instructions of the Client within the scope of order processing, such as careful selection of subcontractors and the agreement of rights to inspection.

Attachment 2 (to Annex 1: AV Contract)

Subcontractor list

Status: May 2, 2024

Subcontractor	Address / Country	Performance
gridscale GmbH	Oskar-Jäger-Str. 173 50825 Cologne Germany	Operation and administration of the IaaS environment through the provision of software and other support services
EXTRA Computer GmbH	Brühlstrasse 12 89537 Giengen an der Brenz Germany	Provision of storage space in the exone.Cloud / Veeam Cloud Backup (VCC)