General Terms and Conditions for trinckle Software Products (“GTCs”)

1. Provider, Subject Matter and Scope

(1) These General Terms and Conditions ("**GTCs**") govern the terms and conditions under which trinckle 3D GmbH, Grimmstraße 12 C, 10967 Berlin, Germany ("**trinckle**") grants the company or department on whose behalf these GTCs are accepted ("**Customer**") the right to use the trinckle software products defined herein ("**Software**").

(2) The Software is intended exclusively for use by businesses (B2B). Use by consumers is explicitly prohibited. By accepting these GTCs on behalf of the Customer, the person accepting these GTCs represents and warrants that they are duly authorized to bind and represent the Customer.

(3) The specific Software covered by these GTCs, the deployment model, and license scope are specified and commercial terms are governed by separate documents from these GTCs:

- in case of Direct Sales by trinckle: the Quote Document provided by trinckle and shared with the Customer
- in case of Reseller Sales: the agreement between the Customer and the reseller
- in case of Online Sales without separate commercial agreements: the terms determined during the online ordering process.

(4) trinckle is not a party to the commercial arrangements between the Customer and the Reseller or the integration partner and has no obligation to intervene in their disputes regarding commercial terms, billing or payment.

(5) The following documents form an integral part of these GTCs:

- Annex A – Service Level Agreement (SLA)
- Annex B – Data Processing Agreement (DPA) pursuant to Art. 28 GDPR

2. Distribution Channels and Contractual Relationships

(1) These GTCs apply regardless of the distribution channel through which the Customer acquires the right to use the Software. The Software may be obtained through:

- Direct Sales: Direct purchase from trinckle; the license is granted directly by trinckle. All commercial terms, billing, and support are governed by trinckle’s Quote Document.
- Reseller Sales: Purchase through an authorized reseller or distributor; the license is granted by trinckle through the reseller. The reseller acts as an intermediary for commercial terms and billing. The Customer's contractual relationship for the use of the Software remains with trinckle under these GTCs.
- Embedded Integration Sales: Access through a third-party software integration platform; the license is granted by trinckle through the integration partner, providing the integrated platform.

(2) The Customer acknowledges that these GTCs create a direct contractual relationship between trinckle and the Customer, irrespective of the distribution channel.

(3) The Customer acknowledges that in case of Embedded Integration Sales, the Software is integrated into the integration partner platform and that the integration partner has its own general terms and conditions governing the use of the integration partner platform. In the event of a conflict between these GTCs and the integration partner's general terms and conditions regarding the use of the Software, these GTCs shall prevail. For all matters relating to the integration partner platform not covered by these GTCs, the integration partner general terms and conditions governing shall apply exclusively. To facilitate distinguishing between the integration partner platform and the Software, the Software is branded as "Powered by trinckle" or by similar means within the integration partner platform.

3. Software Functionality and Limitations

(1) The Software assists the Customer with the creation of high-quality and functional designs. The Software itself does not determine or ensure whether any specific 3D objects or component generated with or through the Software is fit for the Customer's particular intended purpose, functionally operable or of any specific quality, as the suitability and performance also depend on factors beyond trinckle's control, including in particular the Customer's use of the Software, the selected parameters, printers, materials, material combinations and dimensions. Assessing, testing and ensuring for the Customer's intended use remains with the Customer.

(2) trinckle reserves the right to discontinue applications or functionalities of the Software in whole or in part if this is necessary for economic or technical reasons. In such case, trinckle will provide reasonable advance notice to the Customer.

(3) Certain applications or functionalities of the Software under development may be marked as "Beta" or "Early Access" ("**Beta Functionalities**"). Beta Functionalities may be modified or discontinued by trinckle at any time without prior notice.

4. Grant of Usage Rights and Usage Restrictions

(1) trinckle grants the Customer a non-exclusive, non-transferable, and non-sublicensable right to use the Software in accordance with, and within the limits specified in, these GTCs and the applicable commercial agreement.

(2) The Customer is entitled to use the Software exclusively through authorized employees of the Customer and for Customer's internal commercial/business purposes; any use of the Software for personal, consumer or other non-business purposes is excluded.

(3) The Customer is not entitled, without prior written consent from trinckle, to the following activities under these GTCs:

(a) reverse engineering, decompiling, or disassembling the Software, except to the extent necessary to achieve interoperability with an independently created computer program and the information necessary for such interoperability has not been made readily available by trinckle;

(b) reproducing, distributing, renting, or lending the Software in whole or in part, or otherwise granting third parties access to the Software;

(c) circumventing or removing copy protection mechanisms or technical protection measures of the Software;

(d) modifying, altering, or creating derivative works of the Software;

(e) removing or obscuring trademarks, copyright notices or other proprietary marks of trinckle in or on the Software or copies thereof;

(f) using the Software for purposes that violate these GTC's, applicable law or infringe third-party rights.

5. Deployment Models and Technical Requirements

5.1 Cloud Deployment

(1) In case of Cloud Deployment, the Software is hosted on infrastructure operated by third-party cloud service providers and administered by trinckle and is accessible to the Customer via a web browser.

(2) The Customer shall ensure that its users have a stable internet connection and use a current version of a generally supported, market-standard web browser and operating system to access the cloud-based Software.

5.2 OnPrem Deployment

(1) In case of OnPrem Deployment, trinckle provides the Customer with an installable variant of the Software for installation on the Customer's local infrastructure.

(2) The Customer is responsible for the installation, operation, and maintenance of the Software on its infrastructure in accordance with these GTCs.

(3) The Customer shall ensure that its IT infrastructure, including in particular hardware, operating systems, network and security settings, meets the technical requirements specified in the applicable commercial agreement or published by trinckle from time to time on their website.

5.3 Embedded Integration Deployment

(1) In case of Embedded Integration Deployment, the Software is integrated into an integration partner's software solution or platform and is accessible via that platform. The specific form of integration may range from a connection to trinckle's cloud infrastructure as described in Section 5.1 to a full OnPrem integration of the Software within the integration partner's software environment.

(2) The Customer shall ensure that its users meet any technical requirements specified by the integration partner for access to the integration partner's platform. Where the Embedded Integration Deployment involves a connection to trinckle's cloud infrastructure, the Customer shall additionally ensure that its users have a stable internet connection and use a current version of a generally supported, market-standard web browser and operating system.

5.4 No permanent storage of 3D models

In the case of Cloud Deployment and Embedded Integration Deployment that connects to trinckle's administered cloud infrastructure, any designs and 3D models created by the end-user are exclusively processed on trinckle's cloud infrastructure and only for the duration of the active session and are automatically and permanently deleted upon session termination. No design or 3D model data is retained by trinckle beyond the active session. In the case of OnPrem Deployment and Embedded Integration Deployment that is fully integrated, designs and 3D models are processed exclusively on the end-user's local device. No design or 3D model data is received, stored, or retained by trinckle. When selecting an internal storage location for any design or 3D model data, the end-user is responsible for complying with their organization's internal policies, including applicable access rights and authorization concepts.

6. Availability, Support and maintenance

Availability, support and maintenance services are governed by Annex A – Service Level Agreement.

7. Warranty

(1) trinckle warrants that the Software, when used as contractually intended, performs the essential functions as documented in the product description published by trinckle from time to time on trinckle's website trinckle.com/appsuite/product-description. No warranty beyond this is provided.

(2) The warranty relates solely to the conformity of the Software with the essential functions described in the product documentation. In particular, the warranty does not extend to:

- the technical or commercial suitability of the generated 3D objects for Customer's purposes
- uninterrupted or error-free operation of the Software
- compatibility with third-party hardware or software

(3) Notices of defects must be communicated to trinckle in writing without undue delay and described in such a way that trinckle can reproduce the error.

(4) In the event of a defect, trinckle is entitled to provide supplementary performance (*Nacherfüllung*). Supplementary performance may be effected by error correction or delivery of defect-free Software. If supplementary performance fails, the Customer is entitled, at its option, to a reduction of the purchase price or termination of the applicable commercial agreement.

(5) For Cloud Deployment, the warranty period corresponds to the duration of the provision of the Software under the applicable commercial agreement.

(6) For OnPrem Deployment, the warranty period is twelve (12) months from delivery of the Software.

(7) For Beta Functionalities, the warranty is limited. trinckle provides no warranty for the functionality, stability, or completeness of Beta Functionalities.

8. Liability

(1) trinckle's liability is governed by the statutory provisions, unless otherwise provided below.

(2) trinckle is liable without limitation for damages resulting from injury to life, body, or health caused by a negligent or intentional breach of duty by trinckle, its legal representatives, or vicarious agents and for claims under the Product Liability Act and under any guarantees assumed by trinckle.

(3) trinckle is further liable without limitation for damages resulting from an intentional or grossly negligent breach of duty by trinckle, its legal representatives, or vicarious agents, as well as for damages caused by the absence of a guaranteed characteristic.

(4) In case of simple negligence, trinckle is liable only for breach of a material contractual obligation (cardinal obligation). A material contractual obligation is an obligation whose fulfillment is essential for the proper performance of the contract and on whose compliance the Customer may regularly rely. In such case, liability is limited to typically foreseeable damage.

(5) In case of simple negligence, trinckle's liability is limited in amount to the amount received by trinckle from the Customer under the applicable commercial agreement in the twelve (12) months preceding the occurrence of the damaging event.

(6) Except in cases of intent, gross negligence or damage resulting from injury to life, body or health, trinckle shall not be liable for lost revenue, lost profit or other indirect or consequential damages. This shall not affect the Customer’s right to claim compensation for typical, foreseeable damage resulting from a breach of material contractual obligations.

(7) In case of delay in performance for which trinckle is responsible, any claims of the Customer for damages due to such delay shall, in addition to the limitations set out above, be limited to an amount of 20% of the remuneration agreed under the applicable commercial agreement for the delayed service, except in cases of intent or gross negligence.

(8) For Beta Functionalities, trinckle's liability is limited to intent and gross negligence.

(9) The above limitations and exclusions of liability apply to any legal basis of liability and equally to acts and omissions of trinckle, its legal representatives and vicarious agents.

9. Indemnification by Customer

(1) The Customer warrants that it holds all necessary rights to the data, designs and other content it uploads or otherwise inputs into the Software and to the way it uses any output generated by the Software.

(2) The Customer shall indemnify and hold harmless trinckle from and against any third-party claims, damages, costs and expenses (including reasonable legal fees) arising out of or in connection with

- the Customer’s input data or uploaded content infringing third-party intellectual property rights; or
- the Customer’s use of any output generated by the Software in violation of applicable law or third-party rights.

10. Data Protection and Use of Data

(1) Processing as Processor

(a) Where trinckle provides User Management to the Customer, trinckle processes personal data on behalf of the Customer, and the Data Processing Agreement ("DPA") set out in Annex B shall apply.

(b) If the Customer is established outside the European Union, the provisions set out in Annex B, Section V et seq. shall additionally apply, as follows:

- Module 4 of the EU Standard Contractual Clauses, to the extent that personal data processed in the SaaS environment provided by trinckle as part of the Cloud Deployment is transferred back to the Customer; and
- country-specific provisions, where applicable.

The Annexes to the EU Standard Contractual Clauses correspond to those of the DPA and are allocated as follows:

- Annex I.A of the EU Standard Contractual Clauses corresponds to Annex B, Section I of the DPA, with the Processor acting as the data exporter.
- Annex I.B of the EU Standard Contractual Clauses corresponds to Annex B, Section II of the DPA, with the Controller acting as the data importer.

(c) In addition to, and for the avoidance of doubt with respect to, the provisions of Annex B, the following shall apply:

- where written form is required for notices or communications, notice by email to the designated contact person shall be sufficient; and
- in all other respects, the provisions of these GTCs shall apply.

(2) Processing as Controller

(a) In case of Cloud Deployment, trinckle collects and processes usage data (Usage Analytics) for the following purposes as controller:

- Software improvement and product development; legal basis: Art. 6(1)(f) GDPR (legitimate interests) or, where applicable, Art. 6(1)(a) GDPR (consent)
- Analysis of usage frequency and patterns; legal basis: Art. 6(1)(f) GDPR (legitimate interests)
- Detection and resolution of technical issues; legal basis: Art. 6(1)(f) GDPR (legitimate interests)

(b) In case of Direct Sales and independent of the way of deployment, trinckle collects and processes data related to the end-user’s identity (name, email, organization) for billing purposes; legal basis: Billing purposes Art. 6(1)(b) GDPR (performance of a contract)

(c) Information on data subjects’ related rights is available in trinckle's privacy policy at https://www.trinckle.com/privacy.

(5) Use of non-personal data: The Customer agrees that trinckle may use non-personal data which is generated through the use of the Software for

- the performance of a contract or services,
- safety, security and quality ensuring measures,
- support, updates, warranty, guarantee,
- improvement, development and provision of products, services and technologies,
- data centric business models.

trinckle may, in the framework of the above purposes, share data with third parties (service providers, customers, business partners and group companies).

11. Intellectual Property Rights

(1) All rights in the Software, including source code, frontend, scripts, and all other components, belong exclusively to trinckle.

(2) The Customer acquires no ownership rights in the Software. The grant of usage rights occurs exclusively within the scope of these GTCs

(3) The 3D models and configurations created by the Customer using the Software are owned by the Customer. trinckle acquires no rights to such customer results.

(4) The Customer acknowledges that the Software is protected by copyright, design right, and other intellectual property rights.

12. Confidentiality

(1) Each party (the “**Receiving Party**”) agrees to keep confidential all business, technical, or financial information disclosed by the other party (the “**Disclosing Party”**) (“**Cofidential Information**'). Confidential Information of trinckle includes non-public information regarding features, functionality, and performance of the Software. Confidential Information of the Customer includes all information processed by means of the Software, all designs, 3D models, and configurations created by the Customer using the Software (“**Work Results**”), as well as the Customer's business data.

(2) The Receiving Party shall use reasonable care to protect Confidential Information and shall not disclose it to third parties without the Disclosing Party's prior written consent, except as required by law or court order. The Customer agrees that trinckle may disclose Confidential Information to its contractors and sub-processors limited to what is required for the purpose of providing the Software and related services.

(3) Confidential Information does not include information that is or becomes public, was already known to the Receiving Party, is rightfully received from a third party, or is independently developed.

(4) Each party shall ensure that its employees and contractors only have access to Confidential Information to the extent necessary for the performance of the contract (need-to-know) and shall be bound by confidentiality obligations.

(5) The confidentiality obligations shall apply for three (3) years after termination of the contract, except that trade secrets shall remain confidential indefinitely. Upon termination, each party shall return or destroy the other party's Confidential Information upon request.

13. Open-Source Components

(1) The Software contains open-source components that are exclusively licensed under permissive licenses. Copyleft licenses are not used.

(2) A current list of the open-source components used and their licenses is maintained separately by trinckle and is available at https://www.trinckle.com/third-party-notices or upon request.

(3) The open-source components are subject to their respective license terms. In the event of a conflict between the open-source license terms and these GTCs, the open-source license terms shall prevail for the respective component.

14. Term and Termination

(1) The contract term is specified in the applicable commercial agreement.

(2) The right to extraordinary termination for good cause remains unaffected. Good cause exists in particular in case of:

- unpaid due claims despite reminder and setting of a reasonable grace period
- culpable breach of material contractual obligations under these GTCs after unsuccessful reminder
- insolvency, inability to pay, or commencement of insolvency proceedings over the assets of a party

(3) Upon termination of the applicable commercial agreement, the usage right to the Software ceases immediately. In Case of OnPrem Deployment, the Customer shall furthermore delete the Software without delay and destroy or return all copies to trinckle.

(4) trinckle is entitled to assert all outstanding remuneration claims after termination of the applicable commercial agreement. In the case of Reseller Sales or Embedded Integration Sales, trinckle may assert such claims against the reseller or integration partner, as applicable.

15. Export Control

(1) The Customer is responsible for compliance with all applicable export control regulations, including the EU Dual-Use Regulation (Regulation (EU) 2021/821) and national export control laws.

(2) The Software may not be exported, re-exported, or transferred to countries or persons subject to export restrictions or sanctions by the EU, the USA, or other competent authorities within these jurisdictions.

16. Audit Rights

(1) trinckle is entitled, during normal business hours and upon prior notice of three (3) days, to verify the Customer's compliance with the license terms under these GTCs and the applicable commercial agreement.

(2) The Customer shall reasonably support trinckle in conducting the audit and grant trinckle or third-party auditors engaged by trinckle access to the systems and documents that are necessary to verify such compliance, but only to the extent required for this purpose. Any third-party auditors engaged by trinckle must be professionally qualified, must not be direct competitors of the Customer, and must be bound by confidentiality obligations that are at least equivalent to those applicable between trinckle and the Customer.

(3) The audit shall be conducted in a manner that minimally interferes with the Customer's business operations.

(4) If the audit reveals that the Customer has violated the license terms under these GTCs or the terms under the commercial agreement, the Customer shall bear the costs of the audit. Otherwise, each party shall bear its own costs.

17. Force Majeure

(1) Neither party shall be liable for failure or delay in performance of its obligations under these GTCs if such failure or delay is caused by events beyond its reasonable control, including but not limited to acts of God, war, strikes, riots, government actions, or natural disasters ("Force Majeure Event").

(2) The affected party shall promptly notify the other party of the Force Majeure Event and use reasonable efforts to mitigate the effects of such event.

(3) If the Force Majeure Event continues for a period exceeding ninety (90) days, either party may terminate the applicable commercial agreement with immediate effect.

18. Artificial Intelligence

(1) The Software may contain components that use artificial intelligence or machine learning techniques.

(2) trinckle continuously monitors developments in AI legislation and will implement required adaptations to ensure compliance with applicable AI regulations.

(3) The Customer agrees to use any AI functionalities of the Software in accordance with applicable laws and regulations and not for purposes that could violate the rights of third parties.

19. General Provisions

(1) Amendments and supplements to these GTCs require text form. This also applies to the waiver of the text form requirement.

(2) If any provision of these GTCs is wholly or partially invalid or becomes invalid, this does not affect the validity of the remaining provisions. The parties undertake to replace the invalid provision with a valid provision that comes closest to the economic intent of the invalid provision.

(3) These GTCs are governed by the law of the Federal Republic of Germany. The application of the UN Convention on Contracts for the International Sale of Goods (CISG) is excluded.

(4) Exclusive place of jurisdiction for all disputes arising from these GTCs is Berlin, provided the Customer is a merchant, a legal entity under public law, or a special fund under public law. trinckle is, however, entitled to bring an action at the Customer's general place of jurisdiction.

(5) Place of performance is Berlin.

(6) These GTCs contain the complete agreement between the parties regarding the subject matter and replaces all prior agreements, oral or written. Commercial terms are governed by separate agreements as specified in Section 1(4).

(7) trinckle reserves the right to amend these GTCs with notice of six (6) weeks. The Customer may object to the amendment within six (6) weeks of receipt. In the event of an objection, the Customer remains entitled under the old conditions until terminated.

(8) The Customer may transfer its rights and obligations under these GTCs only with prior written consent of trinckle. Consent shall not be unreasonably withheld.

Annex A – Service Level Agreement (“SLA”)

A.1 Applicability

This Annex A forms an integral part of the GTCs and applies to all deployment methods of the Software, with the differences specified below.

A.2 Availability

Cloud Deployment and Embedded Integration Deployment

(1) For Cloud Deployment and Embedded Integration Deployment that connects to trinckle’s administered cloud infrastructure, trinckle provides the Customer with access to the Software. trinckle endeavors to maintain an availability of at least 98.0% on a 24 hours/365 days basis per year. In fully on-premises Embedded Integration scenarios, where the Embedded Integration Deployment does not connect to trinckle’s administered cloud infrastructure, the availability of the overarching integration partner product applies instead of trinckle’s SLA availability under this Annex.

(2) The following periods shall be excluded from the availability calculation:

- Scheduled maintenance windows;
- Unplanned emergency maintenance of up to five (5) hours per year;
- Failures of the server operator;
- Disruptions whose technical causes are not exclusively within trinckle's area of responsibility;
- Force majeure events.

(3) Scheduled maintenance windows shall be announced to the Customer by trinckle at least 48 hours in advance. Scheduled maintenance windows shall typically be performed between 8:00 PM and 6:00 AM CET.

(4) Unplanned downtime will be communicated to the Customer without undue delay.

A.3 Support Services

(1) trinckle furthermore provides installation support for OnPrem Deployment.

(2) trinckle provides first-level support for general inquiries and usage questions in case of Direct Sales. This includes first customer contact and ticket intake, initial troubleshooting and user assistance, classification and prioritization of issues, and collection of all relevant technical information.

(3) For Reseller Sales or Embedded Integration Sales, the Reseller or integration partner is responsible for first-level support, including escalation to trinckle where necessary and justified.

(4) For all distribution channels and deployment methods of the Software, trinckle provides second-level support consisting of analysis of reproducible technical defects in the Software, investigation of confirmed software bugs, provision of workarounds or patches at trinckle’s discretion, and clarification of product behavior and intended functionality.

A.4 Supported Versions

First and Second Level Support in case of OnPrem Deployment and Embedded Integration Deployment is available only if the reported issue occurs in a currently supported release of the Software and can be reproduced in an unaltered version running in a hardware and software environment consistent with the applicable documentation and system requirements.

A.5 Exclusions

trinckle is not obliged under this SLA to:

- provide general user training; any training services may be agreed separately in the applicable commercial agreement
- handle configuration issues not reproducible
- support issues caused by misuse, modifications, or third-party integrations outside trinckle control
- provide real-time or direct end-user support services in distribution models where first-level support is contractually assigned to Resellers or Integration Partners
- support Software that has been (i) used in a manner other than in accordance with the applicable documentation, (ii) repaired, altered, or modified by any party other than trinckle, (iii) improperly installed by any party other than integration partners, its affiliates, or authorized resellers of trinckle or the integration partners, (iv) used with hardware, software, or systems other than those specified in the documentation, to the extent the issue is attributable to such use, or (v) obtained from any entity other than integration partners, its affiliates, or authorized resellers of trinckle or the integration partners
- support any use of the Software directly or indirectly in activities prohibited by applicable EU or U.S. laws

A.6 Support Hours

Support provided by trinckle is available during trinckle's business hours (Monday to Friday, 9:00 AM – 5:00 PM CET or CEST, as applicable), excluding public holidays in Berlin, Germany and trinckle's published holidays.

A.7 Response Handling, Severity Classification and Service Levels
(a) Severity Classification, Initial Response, Communication and Resolution Targets

Severity	Example	Initial Response Time	Target Resolution Timeline (Cloud Deployment)
Severity 1 (Blocker)	Licensed Software fails to start or critical production outage	1 business day	Target resolution or workaround within two (2) business days
Severity 2 (High)	Major functionality unavailable impacting production use	1 business day	Target resolution within three (3) business days
Severity 3 (Medium)	Minor functionality impacted; workaround available; no production blocking impact	2 business days	Target resolution within ten (10) business days
Severity 4 (Low)	General technical questions, minor defects, or cosmetic issues	5 business days	Resolution in next scheduled update, but no less than fifteen (15) business days

For clarity, resolution targets only apply to Cloud Deployment and Embedded Integration Deployment that connects to trinckle's administered cloud infrastructure and are intended as good faith targets based on severity and complexity; however, trinckle shall use commercially reasonable efforts to meet such timelines and prioritize higher-severity issues accordingly. trinckle does not owe any specific resolution times for OnPrem Deployments or in fully on-premises Embedded Integration scenarios but shall use commercially reasonable efforts to resolve errors within a reasonable time, taking into consideration the severity and gravity of the error and the impact it has on the end-users.

A.12 Maintenance

(1) Regular maintenance updates will be provided by trinckle to ensure the security and functionality of the Software.

(2) For Cloud Deployments, updates are automatically installed by trinckle on the servers. The Customer will be informed of planned maintenance windows that might interrupt use of the Software in advance.

(3) For OnPrem Deployments, trinckle makes updates and upgrades available for download. Installation of updates is the responsibility of the Customer. While trinckle highly recommends to always use the latest version of the Software, there is no obligation to install updates.

(4) For Embedded Integration Deployments, updates to the Software are coordinated by trinckle in cooperation with the integration partner. The integration partner is responsible for deploying updates to the integration partner platform.

Annex B – Data Processing Agreement (“DPA”)

STANDARD CONTRACTUAL CLAUSES (EU / EEA)

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28 (3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR).
(b) The controllers and processors listed in **Annex B I** have agreed to these Clauses in order to ensure compliance with Article 28 (3) and (4) GDPR.
(c) These Clauses apply to the processing of personal data as specified in **Annex B II**.
(d) **Annexes B I to IV** are an integral part of the Clauses.
(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of the GDPR.
(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of the GDPR.

Clause 2

Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.
(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

(a) Where these Clauses use the terms defined in the GDPR respectively, those terms shall have the same meaning as in that Regulation.
(b) These Clauses shall be read and interpreted in the light of the provisions of the GDPR respectively.
(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in the GDPR or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 – Optional Docking clause: not applicable

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in **Annex B II**.

Clause7

Obligations of the Parties

7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe the GDPR or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in **Annex B II**, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in **Annex B II**.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in **Annex B III** to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.
(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.
(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from the GDPR. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.
(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.
(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 14 calendar days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.
(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to the GDPR.
(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.
(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of the GDPR.
(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of the GDPR, the processor and the sub-processor can ensure compliance with Chapter V of the GDPR by using standard contractual clauses adopted by the Commission in accordance with of Article 46 (2) GDPR, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.
(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions.
(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:
    (1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;
    (2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;
    (3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;
    (4) the obligations in Article 32 GDPR.

(d) The Parties shall set out in **Annex B III** the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 GDPR, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant (unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);
(b) in obtaining the following information which, pursuant to Article 33 (3) GDPR, shall be stated in the controller's notification, and must at least include:
    (1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
    (2) the likely consequences of the personal data breach;
    (3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

    Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 GDPR, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);
(b) the details of a contact point where more information concerning the personal data breach can be obtained;
(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in **Annex B III** all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations Articles 33 and 34 GDPR.

SECTION III – FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of the GDPR, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:
   (1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;
   (2) the processor is in substantial or persistent breach of these Clauses or its obligations under GDPR;
   (3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to the GDPR.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX B I LIST OF PARTIES

Controller(s): [*Identity and contact details of the controller(s), and, where applicable, of the controller's data protection officer]*

Name: [Customer, cf. to Section 1(1) of the GTCs]

Address: [Customer´s address, as specified in the commercial agreement]

Contact person's name, position and contact details: [if available, as specified in the commercial agreement]

Signature and accession date: [As set out in the commercial agreement]

Processor(s): [*Identity and contact details of the processor(s) and, where applicable, of the processor's data protection officer]*

Name: trinckle 3D GmbH

Address: Grimmstr. 12C, 10967 Berlin, Germany

Contact person's name, position and contact details: Dr. Gunnar Schulze, Chief Technology Officer, privacy@trinckle.com

Signature and accession date: [As set out in the commercial agreement]

ANNEX B II: DESCRIPTION OF THE PROCESSING

Categories of data subjects whose personal data is processed

End-users of the trinckle software (usually: employee of the controller)

Categories of personal data processed

User account data

- Use ID (if provided)
- Email address (if provided)
- Password (if requested; stored as hash, e.g. bcrypt/argon2 – not reversible)
- First name, last name, company name, department / team (if provided)

Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

n. a.

Nature of the processing and purpose(s) for which the personal data is processed on behalf of the controller

Cloud Deployment: In the context of providing/using the software, personal data is processed for user authentication and access control.

Duration of the processing

Cloud Deployment:

- Session data: All customer-related data and 3D model data are deleted after session end. No persistent storage of customer workpiece geometry or configuration results.
- User account data: Account data is generally processed for the duration of contractual relationships and deleted by the processor 30 days after contractual relationships end.

Support Services / OnPrem Deployment:

For processing by (sub-) processors, also specify subject matter, nature and duration of the processing

[as specified above and in **Annex B IV**]

ANNEX B III TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational security measures implemented by the processor and its sub-processor(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons is set out in the following document(s):

- IT Documentation and security aspects: available here: trinckle.com/appsuite/TOM

The controller can sign up for a subscription list to receive notification of updates to the technical and organizational measures implemented: trinckle.com/appsuite/GTC-Updates.

ANNEX B IV: LIST OF SUB-PROCESSORS

The data controller has approved the use of the sub-processors listed in the following document:

- List of Sub-Processors: available here: trinckle.com/appsuite/Sub-Processors.

The controller can sign up for a subscription list to receive notification of changes of the sub-processors: trinckle.com/appsuite/GTC-Updates.

ANNEX B V: EU STANDARD CONTRACTUAL CLAUSES, MODULE 4

STANDARD CONTRACTUAL CLAUSES (processor to controller)

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation (GDPR)) for the transfer of personal data to a third country.The Parties:the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), andthe entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in

Annex I.A (hereinafter each ‘data importer’)have agreed to these standard contractual clauses (hereinafter: ‘Clauses’).

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46 (1) and Article 46 (2) (c) GDPR and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28 (7) GDPR, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of the GDPR.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
    (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
    (ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
    (iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
    (iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
    (v) Clause 13;
    (vi) Clause 15.1(c), (d) and (e);
    (vii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.
(b) Paragraph (a) is without prejudice to rights of data subjects under the GDPR.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in the GDPR, those terms shall have the same meaning as in that Regulation.
(b) These Clauses shall be read and interpreted in the light of the provisions of the GDPR.
(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in the GDPR.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional Docking clause: not applicable

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.
(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.
(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.
(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data (7), the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.
(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter

shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9 – Use of sub-processors n. a. in Module 4

Clause 10

Data subject rights

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under GDPR.

Clause 11

Redress

The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13 – Supervision – n. a. for Module 4

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
   (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
   (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
   (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the

processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
   (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
   (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimization

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under

the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

  (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

  (ii) the data importer is in substantial or persistent breach of these Clauses; or

  (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

  In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45 (3) GDPR that covers the transfer of personal data to which these Clauses apply; or (ii) GDPR becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under GDPR.

Clause 17

Governing law

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Germany.

Clause 18

Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the courts of Germany.

ANNEX B VI: COUNTRY-SPECIFIC PROVISIONS

California Data Processing Addendum

This California Data Processing Addendum ("Addendum") applies to the extent that the processor is Processing controller's California Consumer Personal Information.

(1) Definitions

In this Addendum, "**Regulations**" means applicable regulations promulgated by the California Privacy Protection Agency.

(2) Terms

(a) In addition to existing obligations in the commercial agreement(s) and GTCs, where the processor is a service provider or contractor, as set forth in the CCPA, Section 3 of this Addendum shall apply as applicable and where the processor is a contractor, as set forth in the CCPA, Section 4 of this Addendum shall apply.

(b) Capitalized terms not otherwise defined herein shall have the meaning given to them in the commercial agreement(s) and GTCs or DPA. Wherever the singular is used herein, where the context permits, shall be deemed to include the plural and vice versa. The definition of words in the singular, where context permits, shall be deemed to include the plural and vice versa.

(c) The Parties agree that the controller is a business and the processor is a service provider or contractor in relation to the personal information that is processed in the course of the processor's provision of the business purpose set forth in the commercial agreement(s) and GTCs.

(d) The commercial agreement(s) and GTCs document the business purpose for which the processor is processing personal information. Controller discloses personal information to the processor only for such limited and specified business purpose.

(3) Service Provider and/or Contractor Obligations and Restrictions

(a) In respect of personal information processed in the course of fulfilling the business purpose to controller, the processor:

(i) shall not sell or share personal information it collects pursuant to the commercial agreement;

(ii) shall not sell or share personal information it collects pursuant to the commercial agreement for cross- context behavioral advertising*;*

(iii) shall not retain, use or disclose personal information it collects pursuant to the commercial agreement for any purpose other than the business purpose, or as otherwise permitted by the CCPA and these Regulations;

(iv) shall not retain, use or disclose personal information it collects pursuant to the commercial agreement for any commercial purpose other than the business purpose, unless expressly permitted by the CCPA or the Regulations;

(v) shall not retain, use or disclose personal information it collects pursuant to the commercial agreement outside the direct business relationship between customer and processor, unless expressly permitted by the CCPA or the Regulations. Specifically, the processor shall not combine or update personal information with personal information it has received from another source or collected from its own interaction with the controller, unless expressly permitted by the CCPA or these Regulations*;*

(vi) shall comply with all applicable sections of the CCPA and the Regulations, including—with respect to personal information that it collects pursuant to the commercial Agreement - provision of the same level of privacy protection as required of businesses by the CCPA and the Regulations;

(vii) shall notify controller if the processor determines that it can no longer fulfill its obligations under the CCPA or the Regulations;

(viii) may, subject to the commercial agreement, engage another contractor to assist processor to fulfill the business purpose; provided, however, that the processor must enter into a written agreement with a contractor that complies with this Addendum, the CCPA and the Regulations, including Section 7051(a);

(ix) shall inform controller of any consumer request with which controller must comply, and at controller's request and cost, assist controller with its obligation to respond to verifiable requests from consumers; and

(b) In respect of personal information that controller provides to the processor to fulfill the business purpose, controller has the right, upon advance written notice, to take reasonable and appropriate steps to ensure that the processor uses personal information in a manner consistent with the business's obligations under the CCPA and the Regulations.

(c) If, after completing the assessment described in Section (4), controller determines that the processor may be in violation of its obligations in this Addendum, the CCPA or the Regulations, then upon advance written notice, controller has the right to take reasonable and appropriate steps to stop and remediate processor's unauthorized use of personal information.

(4) Additional Contractor Obligations

Processor certifies that processor understands the restrictions set forth in Section (3) of this Addendum and will comply with them.

(5) Changes in the CCPA

(a) In the event of a change to CCPA whereby the provisions of this Addendum are materially affected or compliance with the terms of this Addendum becomes impractical, the Parties shall negotiate in good faith to agree to an updated Addendum; and

This Addendum is part of the commercial agreement(s) and GTCs between processor and controller, and together with the commercial agreement(s) and GTCs contains the entire agreement of the Parties as to its subject matter. In the event of any direct conflict between this Addendum and the terms and conditions of the commercial agreement(s) and GTCs, this Addendum governs.