

**Data Processing Agreement  
on the Processing of Personal Data by Contract  
("Data Processing Agreement" or "Agreement")**

between

Customer as defined in the GTC

- "Controller" -

And

**NavVis GmbH**  
Blutenburgstr. 18  
D-80636 Munich  
Germany

- „Processor“ -

- Controller and Processor also referred to as "Parties" -

**Preamble**

This Data Processing Agreement supplements the Processor's [GTC](#) and [EULA](#) as updated from time to time between Controller and Processor for the provision of the SaaS services ("**SaaS Services**"). It applies to all activities defined in Section 1.1 including the course of which the Processor's staff processes personal data of the Controller during the provision of the SaaS Services. All capitalized terms in this Agreement shall have the same meaning as in the GTC and EULA if not otherwise defined.

**1. Subject and duration of the Agreement**

1.1. The processing activities carried out by Processor cover the following:

- ☒ Processing data using the IVION Processing on server owned by the Processor or in the NavVis Cloud, hosted on Amazon Web Services (AWS)
- ☒ Processing data using the IVION Processing on server owned by the Controller
- ☒ Hosting data using NavVis IVION or NavVis Cloud on server owned by the Processor, hosted on Amazon Web Services (AWS)
- ☒ Providing Customer Support to Customer

1.2. The assignment specified at 1.1 above solely serves the purpose to operationally process data for which it cannot be excluded that they constitute personal data (Art. 4 no. (1) GDPR) in the context of providing SaaS Services.

1.3. The Processor will process personal data on behalf of the Controller according to Art. 4 no. (2) and Art. 28 GDPR on the basis of this agreement. In case of privacy law related conflict, the provisions of this Agreement shall prevail over the SaaS Services.

1.4. The contractually agreed hosting service will be rendered by the choice of the Controller on a server located in the European Union, Japan or the United States. For applicable additional measures Section 9 applies.

1.5. Any relocation of the service or partial work thereof to a third-party country will require the explicit instruction of the Controller, which may happen through deployment of an instance in the NavVis Cloud and may only take place if the special conditions of Art. 44 et seq. GDPR are satisfied (e.g., adequacy decision of the Commission, standard data protection clauses, approved rules of conduct).

1.6. The term of this agreement is bound to the SaaS Services and is in accordance with the duration of the services agreed under the SaaS Services.

1.7. In case an earlier agreement by the Parties relating to processing of personal data exists, it shall be replaced by this Agreement upon acceptance of the NavVis GTC and/or EULA, unless an individual data processing agreement has been entered into by the Parties.

## 2. Type and purpose of processing, type of personal data and categories of data subjects:

- 2.1. The processing of personal data by contract is limited to the purpose of agreed services and to what is instructed by the Controller (in written form or electronically (e.g. by e-mail; so-called "text form", cf. § 126b German Civil Code).
- 2.2. The Controller's instructions are determined by this Agreement and the SaaS Services.
- 2.3. The purpose of the data processing follows the operational agreements of the service delivery agreed in the SaaS Services.
- 2.4. Type of personal data (according to the definition of Art. 4 No. 1 GDPR) – depending in each case upon instructions and actions of the Controller and potentially its affiliates, partners or clients, and probably comprise: Controller's Data uploaded to the SaaS Services under Controller's SaaS accounts.
- 2.5. Categories of data subjects (according to the definition of Art. 4 No. 1 GDPR) – depending in each case upon instructions and actions of the Controller, and probably comprise and are not limited to:
  - ☒ Supplier of the data Controller
  - ☒ Data Processor's Employees
  - ☒ Persons present at random

## 3. Rights and duties as well as the Controller's authority to give instructions

- 3.1. The Controller alone is responsible for determining the lawfulness of the processing according to Art 6 No 1 GDPR and for upholding the rights of the data subject under Art. 12 to 22 GDPR or according to the data protection laws applicable to the Controller. Nonetheless, the Processor is obligated to forward all such inquiries, in so far as they are discernibly directed exclusively to the Controller, without delay.
- 3.2. Changes to the subject of processing and changes to methods are to be coordinated jointly between Controller and Processor and are to be determined in writing or in a documented electronic format.
- 3.3. The Controller will generally grant all assignments, partial assignments, and instructions in writing or in a documented electronic form. The parties agree that this Agreement, the GTC and the EULA (including Controller providing instructions via configuration tools such as the NavVis Cloud and APIs made available by Processor for the SaaS Services) constitute Controller's documented instructions regarding Processor's processing of Controller Data ("**Documented Instructions**"). Processor will process Controller Data only in accordance with Documented Instructions. Oral instructions are only to be followed by the Processor if they are confirmed without undue delay in writing or in a documented electronic format.
- 3.4. The Controller will notify the processor without undue delay if the Controller notices errors or irregularities when reviewing the assignment results.
- 3.5. The Controller is required to treat as confidential all knowledge obtained during this contractual relationship of data security actions and other business secrets of the Processor and not to provide these to any third party (not even under non-disclosure agreement) without prior written approval of the Processor. This obligation will continue to exist even after termination of this agreement.

## 4. Persons authorized by the Controller to give instructions; persons authorized by the Processor to receive instructions

- 4.1. Controller is solely responsible for ensuring that only sufficiently skilled personnel are allowed to give instructions. Processor shall accept all instructions given by employees or representatives of Controller if no reasonable doubt arises regarding their affiliation to Controller.
- 4.2. Processor has the right to refuse to carry out instructions if there's reasonable doubt about the affiliation with Controller until the affiliation has been cleared.
- 4.3. All employees of Processor are entitled to receive instructions from Controller. Processor shall ensure that only sufficiently skilled personnel are allowed to carry out instructions.
- 4.4. The instructions are to be saved for as long as they are valid and then subsequently for three full calendar years.

## 5. The Processor's duties

- 5.1. The Processor will process personal data solely within the context of providing the SaaS Services and according to the Documented Instructions given by the Controller in so far as the Processor is not required to perform different processing by the law of the Union or the member states to which the Processor is subject (e.g., investigations by prosecutors or state security officials); in such a case, the Processor will communicate these legal requirements to the Controller before the processing work is begun insofar as the relevant law does not prohibit such communication due to an important public interest (Art. 28 (3) clause 2 lit. a GDPR).
- 5.2. The Processor will not use the personal data provided for processing for any other purposes. Copies or duplicates of the personal data will not be made without the Controller's knowledge.
- 5.3. With regard to the Controller's protecting the data subjects rights under Articles 12 to 22 GDPR, creating the records of processing activities, and for necessary data protection impact assessments of the Controller, the Processor has to cooperate as needed and reasonably assist the Controller to the extent possible (Art. 28 (3) sentence 2 (e and f) GDPR). The Processor has to forward the necessary information in each case without delay to the following entity of the Controller: Persons authorized by the Controller to give instructions (as defined in Section 4.1).
- 5.4. The Processor will notify the Controller without delay if in its opinion any instructions given by the Controller violate statutory provisions (Art. 28 (3) sentence 3 GDPR). The Processor is entitled to stop performance of the relevant instructions until said instructions are, following review, confirmed or modified by the Controller's responsible staff.
- 5.5. The Processor has to correct, delete, or limit the processing of personal data based on the contractual relationship if the Controller issues instructions requesting this and this is not opposed by justified interests of the Processor.
- 5.6. The Processor may make disclosures about personal data from the contractual relationship to third parties or the data subject only after prior instructions or consent from the Controller, unless otherwise stipulated by law or court or administrative order.
- 5.7. The Processor hereby agrees that the Controller – generally upon appointment – is entitled to review compliance with the provisions on data protection and data security as well as the contractual agreements, if they concern the subject matter of the SaaS Services, to the extent reasonable and necessary directly or through the Controller's agents which are bound by confidentiality obligations, in particular by obtaining information and inspecting the relevant stored data and data processing programs as well as through audits and inspections on-site (Art. 28 (3) clause 2h GDPR).
- 5.8. The Processor is obliged, to the extent necessary and reasonable, to provide assistance in these reviews.
- 5.9. To the extent that the data is processed in a private residence, access to the employee's residence is to be contractually secured beforehand for the Controller's supervision purposes. The measures under Art. 32 GDPR are also to be ensured in this case.
- 5.10. The Processor agrees to maintain confidentiality concerning the contractual processing of the personal data of the Controller. This will also survive termination of the Agreement for a maximum of ten years.
- 5.11. The Processor will train employees assigned to work under the SaaS Services on the provisions of data protection applicable to them before they begin such work and to oblige them to observe confidentiality in a suitable manner (Art. 28 (3) clause 2 (b) and Art. 29 GDPR). The Processor will monitor compliance with the data protection laws at its company.
- 5.12. For the Processor, Dr. Sebastian Kraska, Marienplatz 2, 80331 Munich, +49 89 1891 7360 is appointed as data protection officer.
- 5.13. The Controller may retrieve the name and contact details of the data protection officer at any time at <https://www.navvis.com/de/privacy-policy>.

## 6. Notification duties of the Processor in the event of processing disruptions and breaches of personal data protection

- 6.1. The Processor will notify the Controller without delay of any disruptions, violations by the Processor or its employees and against data protection laws as well as the suspicion of data protection breaches or irregularities with regard to processing personal data. This mainly applies with regard to any reporting and notification duties of the Controller under Art. 33 and Art. 34 GDPR. The Processor will, if necessary, will reasonably assist the Controller in its duties under Art. 33 and 34 GDPR (Art. 28 (3) clause 2 (f) GDPR).
- 6.2. The Processor may carry out notifications under Art. 33 or 34 GDPR for the Controller only after prior instructions in accordance with Clause 4 of this Agreement.

## **7. Relationships with subcontractors (Article 28 (3) clause 2 (d) GDPR)**

- 7.1. The Processor is permitted to use subcontractors to process the controller's data without further approval by Controller, Art 28 (2), clause 2 GDPR.
- 7.2. The Processor must ensure that it carefully selects the subcontractor based on its qualification while paying particular attention to the suitability of the technical and organizational measures taken by this subcontractor within the meaning of Art. 32 GDPR.
- 7.3. Subcontractors may be used in third countries only if the particular requirements of Art. 44 et seq. GDPR are satisfied (e.g., adequacy decision of the Commission, standard data protection clauses, approved codes of conduct).
- 7.4. The Processor has to contractually ensure that provisions identical or equivalent to the provisions agreed between Controller and Processor also apply to subcontractors. The details are to be set down in the agreement with the subcontractor with such specificity that the responsibilities of the Processor and of the subcontractor are clearly delineated. If multiple subcontractors are used, then this will also apply to responsibilities between these subcontractors. In particular, the Controller must be authorized to carry out reasonable audits and inspections, including on site, of subcontractors as needed, or have such reviews carried out by its agents.
- 7.5. The agreement with the subcontractor must be made in writing, which may also be carried out in an electronic format (Art. 28 (4) and (9) GDPR).
- 7.6. Currently, the subcontractors designated in Annex 1: Subcontractors for the processing of personal data, by name, address, and assignment contents are being used on behalf of the Processor for the processing of personal data to the extent named therein.
- 7.7. The Processor will notify the Controller about any intended change regarding the addition of new or replacement of existing subcontractors.
- 7.8. The Controller has the option to objection to such change, if the technical and organizational measures previously agreed upon cannot, in essence, be fully met. In such case the intended change must not be executed.

## **8. Transfers of Personal Data.**

- 8.1. Regions. Controller can specify the location(s) where Controller Data will be hosted within the AWS Network (each a "Region"), including Regions in the EEA, Japan and USA. Once Controller has made its choice, Processor will not transfer Controller Data from Controller's selected Region(s) except as necessary to provide the Services initiated by Controller, or as necessary to comply with the law or valid and binding order of a governmental body.
- 8.2. Application of Standard Contractual Clauses. Subject to Section 8.1, the Standard Contractual Clauses will only apply to Controller Data subject to the GDPR that is transferred, either directly or via onward transfer to a country outside the EEA not recognized by the European Commission as providing an adequate level of protection for personal data as described in the GDPR ("Third Country" and each a "Data Transfer").
- 8.3. When Controller is acting as a controller, the Controller-to-Processor Clauses will apply to a Data Transfer.

## **9. Technical and organizational measures under Article 32 GDPR (Art. 28 (3) clause 2 (c) GDPR )**

- 9.1. For the specific contractual processing, a protection level that is commensurate with the rights and freedoms of the natural persons affected by the processing is guaranteed. To that end, the protective goals of Art. 32 (1) GDPR , such as confidentiality, integrity, and availability of the systems and services as well as their reliability regarding the type, scope, circumstances, and purchase of the processing work are to be taken into account such that appropriate technical and organizational remedies will permanently limit risk.
- 9.2. The data protection plan described in Annex 2: Data Protection Policy shows the selection of the technical and organizational measures appropriate to the determined risk while taking into account the protective goals according to the latest technical standards in detail and while paying particular attention to the IT systems and processing procedures that the contractor uses.
- 9.3. It also describes the method for regular review, assessment and evaluation of the effectiveness of the technical and organizational measures to ensure legally compliant processing of personal data.
- 9.4. The Processor has to regularly test, assess and evaluate the technical and organizational measures to ensure the security of the processing (Art. 32 (1) (d) GDPR).
- 9.5. The Processor's actions can be adapted over the course of the contractual relationship for technical and organizational further development but may not fall below the agreed standards.
- 9.6. The Processor must coordinate substantial changes with the controller in documented form (in writing, electronically). Records of such coordination efforts are to be stored for the duration of this agreement.

## **10. Processor's obligations after termination of the assignment, Art. 28 (3) sentence 2 (g) GDPR**

- 10.1. Upon completing the contractual work, the Processor shall, at the discretion of the Controller,
  - 10.1.1. deliver to the Controller all data, records, and created processing or usage results obtained by the Processor or subcontractors and that relate to the contractual relationship,
  - 10.1.2. or delete or destroy in a manner conforming to data protection laws.
- 10.2. In case the Controller has not chosen one of the above alternatives within three months from finalization of the processing activities, the data shall be deleted.
- 10.3. Confirmation of deletion or destruction is to be sent to the Controller up on request in writing or in a documented electronic format.

## **11. Miscellaneous**

- 11.1. Agreements on the technical and organizational measures as well as the review and audit records (including for subcontractors) are to be stored by both contractual parties for as long as they are valid and then subsequently for three full calendar years.
- 11.2. Written form or documented electronic format is generally required for supplemental agreements.
- 11.3. This Agreement is made under the substantive laws of the Federal Republic of Germany. To the extent legally permissible, the courts of Munich, Germany shall have exclusive jurisdiction.
- 11.4. The Processor shall notify the Controller without undue delay if the Controller's property or personal data to be processed are jeopardized by third-party actions at the Processor's (for instance through seizure or confiscation) by bankruptcy or settlement proceedings, or by any other events.
- 11.5. The defense of the right to retention within the meaning of Section 273 German Civil Code ("BGB") is excluded with regard to the data processed for the Controller and the pertinent data media.
- 11.6. If individual parts of this Agreement should be invalid, then this will not otherwise affect the validity of the Agreement.

### **Annex 1**

Amazon Web Services EMEA SARL., 38 avenue John F. Kennedy, L-1855 Luxembourg  
Hosting, processing.

### **Annex 2**

Available upon request.