# Data processing agreement pursuant to Art. 28 GDPR

This Data processing agreement is concluded between

*[insert: Company name and address of the Controller]*

(hereinafter referred to as “Controller”)

and

*[insert: Company name and address of the Processor]*

(hereinafter referred to as “Processor”)

The Processor commits himself to provide the data processing described hereinafter within the meaning of Art. 4 Nr. 2 and Art. 28 GDPR on behalf of the Controller. For the purposes of this Data processing agreement the definitions of the General Data Protection Regulation (GDPR, Regulation (EU) 2016/679) apply.

## I. Subject and Duration of the Contract

## Subject

## The agreement includes the following:

*(Subject of the agreement, detailed description of the data processing)*

**Duration**

### This agreement begins on ................................... and ends on ................................................

or

This agreement is concluded for an indefinite period of time and can be terminated by either party with a notice of ...... [*enter period of notice, e.g. one month] to ....... [enter termination date, e.g. calendar quarter*].

The Controller may terminate the agreement at any time without notice in the event of a serious breach by the Processor of data protection regulations or the provisions of this agreement, if the Processor cannot or does not want to carry out an instruction of the Controller or the Processor denies control rights of the Controller in violation of the contract. In particular, failure to comply with the obligations agreed in this agreement and obligations derived from Art. 28 GDPR constitutes a serious breach.

## II. Place of data processing, categories of personal data, categories of data subjects, nature and purpose of processing

|  |
| --- |
| Place of data processing All data processing activities are carried out exclusively within the EU or EEA.  Option: Data processing activities are also carried out, at least partly, outside the EU or EEA, namely in ..... [enumerate countries]. The appropriate level of data protection results from [options, please delete as appropriate]:   * An adequacy decision of the European Commission according to Art. 45 GDPR. * An exception for the specific case pursuant to Art. 49 para. 1 GDPR. * Binding internal data protection rules pursuant to Art. 47 in conjunction with Art. 46 para. 2 letter b GDPR. * Standard data protection clauses according to Art. 46 para. 2 letter c and d GDPR. * Approved rules of conduct according to Art. 46 para. 2 letter e in connection with Art. 40 GDPR. * An approved certification mechanism according to Art. 46 para. 2 letter f in connection with Art. 42 GDPR. * Contract clauses approved by the data protection authority in accordance with Art. 46 para. 3 letter a GDPR. * an exception for the individual case according to Art. 49 para. 1 subparagraph 2 GDPR.  Categories of data in accordance with Art. 4 no. 1 GDPR The personal data belong to the following data categories (please specify): |
| optional: **Categories of sensitive data in accordance with Art. 4 no. 13, 14 and 15 GDPR**  The personal data comprises the following sensitive data: |
| Categories of data subjects The personal data concern the following categories of data subjects concerned: |
| Type of processing in accordance with Art. 4 no. 2 GDPR The personal data is subject to the following basic processing measures: |
| Purposes of processing The personal data will be processed for the following purposes determined by the Controller: |

## III. Obligations of the Processor

1. The Processor shall process personal data exclusively in accordance with the contractual provisions of this agreement or as instructed by the Controller in a documented manner, unless the Processor is legally obliged to further process the data. The Processor shall notify such obligations to the Controller prior to processing, unless the law concerned prohibits such notification on the grounds of an important public interest (Art. 28 para. 3 sentence 2 letter a GDPR).
2. Unconditional compliance with the instructions of the Controller shall in particular also apply with regard to the transfer of personal data to a third country or international organization, unless the Processor is obliged to do so by the law of the Union or of the Member State to which the Processor is subject. In such a case, the Processor shall inform the Controller of these legal requirements prior to processing, unless the law concerned prohibits such notification for an important public interest.
3. The instructions are initially set out in the agreement and may subsequently be amended, supplemented or replaced by individual instructions in writing or in an electronic format (text form) by the Controller to the Processor (individual instruction).
4. Oral instructions shall be confirmed immediately in writing or in text form.
5. The Processor shall not use the data provided for processing for any other purposes, in particular not for his own purposes. Copies or duplicates of the personal data shall not be made without the consent of the Controller. This does not apply to technically necessary, temporary duplications, provided that an impairment of the data protection level agreed here is excluded.
6. The Processor strictly separates the data to be processed within the scope of this agreement from other data stocks.
7. In the context of data processing, the Processor shall observe the relevant general data protection regulations. The Processor confirms that the persons employed by him for data processing are familiar with the relevant provisions of data protection and this agreement. Corresponding training and sensitization measures shall be carried out at regular intervals.
8. The Processor declares in a legally binding manner that he has obligated all persons entrusted with the data processing to maintain confidentiality prior to commencement of the activity or that they are subject to an appropriate legal obligation to maintain confidentiality. In particular, the obligation of confidentiality of the persons entrusted with data processing shall remain in force even after termination of their activities and end of their employment with the Processor.
9. Optional: He also undertakes to observe the following confidentiality obligations relevant for this order, which are incumbent on the Controller: .......................................................(e.g. banking secrecy, professional secrets, etc.)

1. The Processor shall support the Controller to the extent necessary in granting the rights of the data subjects in accordance with Articles 12 to 22 GDPR. If a data subject sends a request directly to the Processor, the Processor will immediately forward the request to the Controller. The Processor may only provide information to third parties or data subjects with the prior consent of the Controller.
2. The Processor assists the Controller in complying with the obligations set out in Articles 32 to 36 GDPR (data security measures, notification of violations of personal data protection to the supervisory authority, notification of the person affected by a violation of personal data protection, data protection impact assessment, prior consultation).
3. If the Controller is subject to an inspection by supervisory authorities or other bodies, the Processor shall provide the Controller with the necessary assistance to the extent that the order processing is affected.
4. The Processor shall inform the Controller immediately if, in his opinion, an instruction issued violates legal regulations. The Processor is entitled to suspend the execution until the relevant instruction is confirmed or changed by the Controller after verification to this end.
5. The Processor shall rectify or delete personal data from the contractual relationship or restrict its processing if the Controller so requests and no legitimate interests of the Processor prevent this.
6. According to Art. 37 GDPR, Mr. / Mrs. .............................................. [enter: first name, surname, organizational unit, telephone, e-mail] has been appointed as data protection officer by the Processor. The Processor shall inform the Controller immediately if the person who is appointed as the data protection officer changes.

Or: The Processor has not appointed a data protection officer, as there is no legal requirement for such appointment. The contact person for data protection issues at the Processor is Mr. / Ms. [enter: first name, surname, organizational unit, telephone, e-mail].

Optional: If the Processor is not established in the EEA, .............................................. [Enter: name, organization, telephone, e-mail] is appointed as the responsible contact person ("Representative") in the EEA pursuant to Art. 27 GDPR. If the person appointed as representative changes, this shall be communicated to the Controller without delay.

## IV. Sub-processors (Art. 28 para. 2 GDPR, Art. 28 para. 3 sentence 2 letter d GDPR)

Option 1

1. The Processor shall not appoint any sub-processor unless authorized by the Controller in the individual case.
2. The Controller agrees that the sub-processors named in the appendix ...... will be working for the Processor. The nature and scope of their data processing are also defined in annex ......
3. The same data protection obligations as set out in the agreement between the controller and the processor shall apply to sub-processors.
4. On request, the Controller shall be granted access to the relevant agreements between the Processor and the sub-processor.
5. The Controller is entitled to carry out checks at any time, to the extent specified here, also on sub-processors or to have them carried out by third parties.
6. The responsibilities of the Processor and sub-processor shall be clearly separated.
7. If the sub-processor fails to comply with his data protection obligations, the Processor shall be liable to the Controller for compliance with the sub-processor’s obligations.

Option 2:

1. The Processor is authorized to engage another sub-processor at any time.
2. The Controller shall be notified of the engagement before awarding the contract.
3. According to Art. 28 para. 2 GDPR, the Controller has the right to object to this engagement.
4. In the case of an objection ...... (As the GDPR does not regulate the consequences of this objection, it is recommended that these be stipulated in a contract. If no provision is made, the appointment of the sub-processor against whom objection has been raised is not possible).
5. Points 3-7 in option 1 also apply if option 2 is chosen.

Option 3:

The Processor is not entitled to engage a sub-processor.

## V. Technical and organizational measures

1. The Processor shall take all necessary measures to ensure the security of the processing in accordance with Art. 32 GDPR. The measures shall ensure a level of protection appropriate to the risk in terms of confidentiality, integrity, availability and the resilience of the systems. The state of the art, the implementation costs and the nature, scope and purposes of the processing as well as the varying probability of occurrence and severity of the risk to the rights and freedoms of natural persons within the meaning of Art. 32 para. 1 GDPR must be taken into account.
2. The necessary technical and organizational measures are specified in appendix ..... to this contract.
3. Important changes shall be documented immediately.
4. If the security measures taken do not or no longer meet the requirements of the Controller, the latter shall notify the Processor.

## VI. Obligations of the Processor after termination of the agreement (Art. 28 para. 3 sentence 2 letter g GDPR)

1. Upon termination of the data processing, the Processor shall return all the personal data as well as copies thereof to the Controller [or, alternatively] to delete them on the Controller's behalf, unless an obligation to store the personal data exists under Union or Member State law. The return of the copies resp. the completion of the deletion process must be confirmed in writing.

(2) If the Processor processes the data in a special technical format, he shall return the data after the termination of this agreement either in this format or, at the request of the Controller, in the format in which he received the data from the Controller or in another, common format.

**VII. Rights and Obligations of the Controller**

**The Controller is entitled**

(1) to check compliance with the technical and organizational measures taken by the Processor and with the obligations laid down in this agreement, either himself or through third parties on site to an appropriate extent. The persons entrusted with the inspection shall be granted access and insight by the Processor as far as necessary. The Processor shall provide the necessary information.

(2) Inspections at the Processor's premises shall be carried out without any avoidable disruption of his business operations and, except for urgent reasons, after reasonable notice and during the business hours of the Processor.

**The Controller is obliged**

1. to ensure that the processing is lawful in accordance with Art. 6 para. 1 resp. Art. 9 para. 2 GDPR;
2. to ensure that the rights of the data subjects according to Articles 12 to 22 GDPR are respected. However, if only the Processor has the competence to respond to the requests, the Controller will immediately forward the requests to him;
3. to submit instructions to the Processor in writing or in a documented electronic format, as a rule. Oral instructions shall be confirmed in writing or in a documented electronic format;
4. to inform the Processor immediately of any errors or irregularities in the examination of the order results;
5. to treat all information of business secrets and data security measures of the Processor obtained within the scope of the contractual relationship as confidential. This obligation shall remain in force after the termination of this agreement.

## VIII. Liability

Reference is made to Art. 82 GDPR.

Option: Own agreement between the parties

## IX. Miscellaneous

To be supplemented individually

**Signatures**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| Place and Date | Place and Date |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| Controller | Processor |

**All measures to be taken must be specified in a contract in concrete form - general statements and repetitions of the legal regulations are not sufficient for this purpose.**

**Below you will find explanations and examples of the measures required by law. Please specify them according to the circumstances in your organization!**

## 1. Confidentiality (Art. 32 para. 1 letter b GDPR)

* **Physical access control**

No unauthorized access to data processing systems, e.g. magnetic or chip cards, keys, electric door openers, plant security or gatekeepers, alarm systems, video systems;

* **Access rights**

No unauthorized system use, e.g. (secure) passwords, automatic locking mechanisms, two-factor authentication, encryption of data media;

* **Access control**

No unauthorized reading, copying, modification or removal within the system, e.g. Authorization concepts and needs-based access rights, logging of accesses;

* **Separation control**Separate processing of data collected for different purposes, e.g. multi-client capability, sandboxing;
* **Pseudonymization** (Art. 32 para. 1 letter a GDPR; Art. 25 para. 1 GDPR)

The processing of personal data in such a way that the data can no longer be assigned to a specific data subject without the inclusion of additional information, provided that this additional information is kept separately and is subject to appropriate technical and organizational measures.

## 2. Integrity (Art. 32 para. 1 letter b GDPR)

* **Transmission control**No unauthorized reading, copying, modification or removal during electronic transmission or transport, e.g. encryption, Virtual Private Networks (VPN), electronic signature.
* **Entry control**Determining whether and by whom personal data have been entered, modified or removed from data processing systems, e.g: logging, document management.

**3. Availability and resilience (Art. 32 para. 1 letter b GPDR)**

* **Availability control**Protection against accidental or wilful destruction or loss, e.g. backup strategy (online/offline; on-site/off-site), uninterruptible power supply (UPS), virus protection, firewall, reporting channels and emergency plans;
* Rapid restorability (Art. 32 para. 1 letter c GDPR).

## 4. Procedures for regular review, assessment and evaluation (Art. 32 para. 1 letter d GDPR; Art. 25 para. 1 GDPR)

* Data protection management;
* Incident-Response-Management;
* Privacy-friendly default settings (Art. 25 para. 2 GDPR);
* Order control  
  No order data processing in the sense of Art. 28 GDPR without corresponding instruction of the Controller, e.g. clear contract drafting, formalized order management, strict selection of the service provider, obligation to assure in advance, follow-up checks.