Contract processing agreement according to Art. 28 (3) GDPR

effective date 31.08.2024 - translation

1. Introduction and Contracting Parties

This contract was created according to the template for a contract processing contract under Art. 28 (3) GDPR (see https://www.lda.bayern.de/media/muster/formulierunghilfe_av.pdf).

The Contracting Parties shall be Laware ("supplier") and the User of the Laware Service ("client") as under the General Terms and Conditions of Laware.

2. Subject matter and duration of the agreement

The order shall include:

Provision of services to simplify work with legal texts on the Internet. A specific description is given by the general terms and conditions or individual contracts concluded between the parties, in which this contract processing contract is included ("main contract").

(Company of the contract, specific description of services)

The supplier may process personal data for the client in the sense of Art. 4 No 2 and Article 28 GDPR on the basis of this contract.

The contractually agreed service shall be provided exclusively in a Member State of the European Union or in a Contracting State to the Agreement on the European Economic Area. Any transfer of the service or partial work to a third country requires the prior consent of the client and may only take place if the specific conditions of Article 44 et seq. GDPR (e.g. Commission adequacy decision, standard data protection clauses, approved rules of conduct).

Duration of the order

The contract is concluded indefinitely. The term is determined according to the term of the main contract.

The client may terminate the contract at any time without having to comply with a period of time when supplier's serious breach of the data protection regulations or the provisions of this contract is present, the supplier cannot or is not willing to carry out or the supplier refuses control rights of the client contrary to the contract. In particular, the non-compliance with Art. 28 GDPR is a serious violation.

3. Type and purpose of processing, type of personal data and categories of data subjects

Type of processing (corresponding to the definition of Art. 4 No. 2 GDPR):
Collection, storage, modification, reproduction and deletion of data.

Type of personal data (corresponding to the definition of Art. 4 No. 1, 13, 14 and 15 GDPR):

- IDs
- Name
- Address
- E-mail addresses
- Professional designations (optional)
- Company name (optional)
- Time stamp (approximately created, modified etc.)
- Password Hashes
- All data that the user uploads to the services (e.g. comments or other texts)

Categories of persons affected (corresponding to the definition of Article 4(1) GDPR):

- Data from user employees

4. Rights and obligations as well as instructions of the client

For the assessment of the admissibility of the processing in accordance with Art. 6 (1) GDPR, as well as for the protection of the rights of the data subjects according to Art. 12 to 22 GDPR alone the client is responsible. Nevertheless, the supplier is obliged to forward all such requests without delay, provided that they are clearly directed exclusively to the client.

Changes in the subject-matter and procedural changes shall be agreed jointly between the client and the supplier and shall be determined in writing or in a documented electronic format.

The client shall in principle issue all orders, subcontracts and instructions in writing or in a documented electronic format. Oral instructions shall be confirmed immediately in writing or in a documented electronic format.

The client shall be entitled, as defined in 6., to assess before the start of processing and then regularly in a reasonable manner the compliance with the technical and organisational measures taken by the supplier and with the obligations laid down in this contract.

The supplier shall inform the client immediately if it establishes errors or irregularities in the examination of the order results. The client is obliged to treat all the knowledge acquired under the contractual relationship of the clients's business secrets and data security measures confidentially. This obligation shall also remain after the termination of this contract.

5. Persons with right to instruct on client-side, recipient of the supplier

The person entitled to instructions of the client is the user as indicated in the registration for the service.

The recipient is the person mentioned in the legal notice of the website https://laware.de.

Communication channels to be used for instructions: Laware services. Further instructions by email are only permitted if their goals are not covered by the functions of the software.

In the event of a change or a longer-term prevention of the contact persons, each party shall inform the other party immediately and in principle in writing or electronically of the successors or representatives. The instructions shall be kept for their validity and subsequently for three full calendar years, unless they are granted by the operation of technical functions of platforms.

6. supplier's obligations

The supplier shall process personal data exclusively within the framework of the agreements concluded and after instructions provided by the client, provided that it is not obliged to do so for any other processing by the law of the Union or the Member States to which the processor is subject (e.g. investigations of law enforcement or State protection authorities); in such a case, the processor shall inform the controller of these legal requirements before processing, provided that the relevant right does not prohibit such a communication because of an important public interest (Art. 28 para. 3 sentence 2 lit. a GDPR). The instructions are in principle determined by the contracts concluded between the parties and the functions of the software. This does not exclude any additional instructions which the client may provide to ensure the compatibility with the relevant data protection law.

The supplier does not use the personal data left for processing for any other, in particular not for its

own purposes. Copies or duplicates of the personal data are not created without the knowledge of the client. The supplier shall ensure that all agreed measures are implemented in accordance with the contract in the field of the processing of personal data according to the contract. It shall ensure that the data processed for the client are strictly separated from other data. The data carriers that originate from or are used for the client are particularly marked. Entrance and exit as well as the current use are documented. The supplier shall, in particular, carry out the following measures for the client over the entire processing of the service:

- See Data Protection Concept (16.)

The result of checks shall be documented.

In the fulfilment of the rights of the persons concerned pursuant to Art. 12 to 22 GDPR by the client, in the creation of the directories of processing activities and in the case of necessary data protection impact assessments by the client, the supplier shall cooperate to the extent necessary and shall assist the client as appropriate as possible (Art. 28 para. 3 sentence 2 lit e and f GDPR). It shall forward the necessary information to the client immediately:

- Contact details of the user as specified in the registration.

The supplier shall immediately inform the client if, in his opinion, a instructions issued by the client violates legal provisions (Art. 28 para. 3 sentence 3 GDPR). Supplier is entitled to suspend the execution of the corresponding instructions until it is confirmed or changed by the responsible person at the client after verification.

Supplier shall correct, delete or restrict the processing of personal data from the contractual relationship if the client requires this by means of instructions and does not object to the legitimate interests of the supplier.

Information about personal data from the contract relationship to third parties or the data subject may only be provided by supplier upon prior instructions or consent of the client.

The supplier agrees that the client - in principle in accordance with an appointment agreement - is entitled to monitor compliance with the provisions relating to data protection and data security as well as the contractual agreements to a reasonable and necessary extent, or by third parties commissioned by the client, in particular by obtaining information and access to the stored data and the data processing programs as well as by checking and inspections on site (Art. 28 (3) (2) (h) GDPR). All costs incurred shall be borne by the client.

The supplier shall ensure that, where necessary, it assists in these checks. For this purpose, the following is agreed:

Insofar as data are processed in a private apartment, access to the housing of the employee must be contractually guaranteed for the purpose of controlling the employer. The measures referred to in Art.

32 GDPR must also be ensured in this case.

The supplier confirms that the data protection regulations of the GDPR relating to the processing of orders are known to him.

The client undertakes to maintain confidentiality when processing the personal data of the client in accordance with the contract. This will continue after the end of the contract.

The supplier shall ensure that he familiarises the employees involved in the performance of the work with the provisions of data protection which are relevant to them before the commencement of the activity and, in a suitable manner, obliges them to remain silent for the time of their activity and after the termination of the employment relationship (Art. 28 (3) (2) (b) and Art. 29 GDPR). The supplier monitors compliance with data protection regulations in its operation.

An operational data protection officer is not appointed to the supplier, as the legal necessity is not present.

7. Notification obligations of the supplier in the event of malfunctions of the processing and in the event of breaches of the protection of personal data

The supplier shall immediately inform the client of any malfunctions, violations of the supplier or of the persons employed by him or against data protection regulations or the provisions on behalf, as well as the suspicion of data protection violations or irregularities in the processing of personal data. This applies, in particular, to the client's reporting and notification obligations under Art. 33 and 34 GDPR. The supplier is obliged to support the client, if necessary, regarding its obligations under Art. 33 and 34 GDPR (Art. 28 (3) (2) (f) GDPR). Reports by Art. 33 or 34 GDPR for the client, the supplier may only conduct after prior instructions pursuant to No. 4 of this contract.

8. Subcontracting with subcontractors (Art. 28 (3) (2) (d) GDPR)

The client shall grant the supplier a general authorisation for the commissioning of subcontractors for the processing of data of the client as described below.

The supplier shall communicate to the client the name and address and the intended activity of the subcontractor. In addition, the supplier must ensure that the subcontractor takes particular account of the suitability of the technical and organisational measures taken by that subcontractor within the meaning of Article 32 GDPR carefully selected. The relevant test documents must be made available to the client on request.

Subcontracting in third countries may only be carried out if the specific requirements of Article 44 et seq. GDPR are met (e.g. Commission adequacy decision, standard data protection clauses, approved rules of conduct).

The supplier shall contractually ensure that the agreed arrangements between client and supplier also apply to subcontractors. In the contract with the subcontractor, the information shall be so specific

that the responsibilities of the supplier and the subcontractor are clearly defined from each other. Where several subcontractors are employed, this shall also apply to the responsibilities between those subcontractors. In particular, the client must be entitled to carry out appropriate checks and inspections, including on-site, for subcontractors or to have them carried out by third parties commissioned by him.

The contract with the subcontractor must be written in writing, which can also be done in an electronic format (Art. 28 (4) (9) GDPR).

The transmission of data to the subcontractor shall not be permitted unless the subcontractor fulfils the obligations under Art. 29 and Art. 32 (4) GDPR with regard to its employees.

The supplier shall verify compliance of the subcontractor(s)' obligations.

The supplier shall be liable to the client for the subcontractor to comply with the data protection obligations imposed by the supplier in accordance with this section of the contract.

At present, the subcontractors referred to in 15. are hired by the supplier for the processing of personal data to the extent specified therein.

The client agrees with their assignment.

The processor shall always inform the controller of any intended change in relation to the addition of new subcontractors or the replacement of previous subcontractors, thereby allowing the client to object to such changes (Art. 28 (2) (2) GDPR).

9. Technical and organisational measures under Art. 32 GDPR (Art. 28 (3) (2) (c) GDPR)

A level of protection appropriate to the rights and freedoms of natural persons affected by the processing shall be ensured for specific order processing. For this purpose, the protective objectives of Art. 32 para. 1 GDPR, such as confidentiality, integrity and availability of the systems and services, as well as their resilience with regard to the nature, scope, circumstances and purpose of the processing, in such a way that appropriate technical and organisational corrective measures are used to mitigate the risk over time.

The data protection concept described in 16. represents the selection of technical and organizational measures to suit the identified risk, taking into account the protection objectives according to the state of the art, in detail and with particular consideration of the IT systems and processing processes used by the supplier.

Decisions concerning the organisation of data processing and the procedures used must be made between supplier and client.

Where the measures taken by the supplier are not sufficient to meet the requirements of the client, it

shall notify the supplier immediately.

The measures taken by the supplier may be adapted to the technical and organisational development in the course of the contract, but may not fall below the agreed standards.

The supplier must discuss with the client significant changes in documented form (written, electronic). Such discussions shall be kept for the duration of this contract.

10. Suppliers's obligations after termination of the contract, Art. 28 (3) (2) (g) GDPR

After completion of the contractual work, the supplier shall delete or delete all data, documents and processing or use results relating to the contractual relationship as follows: to be destroyed/destroyed: the deletion or destruction must be confirmed to the client in writing or in a documented electronic format with a date indication.

11. Payment

An agreed compensation is held in the main contract or in the general terms and conditions.

12. Liability

Art. 82 GDPR and the main contract including the general terms and conditions are referred to.

13. Penalties

No contractual penalty is agreed.

14. Other

Agreements on technical and organisational measures and control and audit documents (including subcontractors) shall be retained by both parties for their validity and subsequently for three full calendar years.

In principle, the font or a documented electronic format is required for secondary agreements.

The objection of the right of retention i. S. v. § 273 BGB is excluded with regard to the data processed for the client and the associated data carrier.

If individual parts of this Agreement are ineffective, this shall not affect the validity of the Agreement.

15. Annex 1: Processors used

The supplier shall use the following subcontractors:

- goneo Internet GmbH, Dresdener Strasse 18, 32423 Minden: Provision of Laware Website and Apps

(Hosting)
- Strato AG, Otto-Ostrowski-Straße 7, 10249 Berlin: Provision of additional services (e.g. translation)

16. Annex 2: Data protection concept

16.1 Pseudonymisation and encryption of personal data

- Laware takes care to store personal data only pseudonyms at different locations, as far as this is technically possible and meaningful.
- Passwords are only saved in a hashed. A hash algorithm corresponding to the prior art is used.
- E-mail addresses in texts to be publicly displayed are rendered unmistakable in the source text as far as possible.
- Data between users, visitors and servers are transmitted encrypted. The TLS 1.3 protocol is currently being used.
- Sensible tokens or keys are also encrypted.

16.2 Ability to ensure the confidentiality, integrity, availability and resilience of systems and services related to processing over time

- Data stored in premises of Laware (e.g. test systems) are operated on a server with uninterrupted power supply.
- Laware's premises are secured with electronic locking device.
- Passwords that correspond to the current recommendations of the BSI are selected.
- The data sets of different customers are treated separately.
- Software on productive systems is used on managed servers to ensure the topicality of important basic systems.
- The loadability of the systems is checked in a random manner and on special occasions.
- Software is stored and developed in repositories

16.3 to quickly restore the availability of personal data and access to them in a physical or technical incident

- Of the databases, regular backups are created by both the service provider and Laware

16.4 Procedure for regular review, evaluation and evaluation of the effectiveness of technical and organisational measures to ensure the safety of processing

- The measures are regularly examined and supplemented.

Laware.de Document Identifier: 040fb4ea-4212-11ef-b89e-1866da5b199e/b84c9ec4-678f-11ef-8509-320482972007/tr-en/2024-09-20-06-14