

Contract for order processing according to Art. 28 GDPR Agreement

between

.....
person responsible - hereinafter referred to as the client –

and

caesar data & software GmbH, Hindelanger Straße 35, 87527 Sonthofen

processors - hereinafter referred to as contractors

1. Subject and duration of the contract

(1) Subject

The subject of the data handling order is the performance by the contractor of the following tasks: performance of maintenance work to adapt, assist or correct the software supplied by the contractor.

(2) Duration

The contract is open-ended and can be terminated by either party at the end of the year with six months' notice. This does not affect the possibility of termination without notice.

2. Specification of the content of the order

(1) Nature and purpose of the intended processing of data

Detailed description of the subject matter of the order with regard to the type and purpose of the contractor's tasks: adaptation, assistance or correction of the software with regard to questions, change requests or complaints of the client.

The provision of the contractually agreed data processing takes place exclusively in a member state of the European Union or in another state party to the Agreement on the European Economic Area. Any transfer to a third country requires the prior consent of the principal and may only take place if the special requirements of Art. 44 ff. GDPRs are fulfilled.

(2) Type of data

The subject of the processing of personal data are the following data types/categories

- a) Person master data
- b) Communication data (e.g. telephone, e-mail)
- c) Contract master data (contractual relationship, product or contractual interest)
- d) Customer history
- e) contract billing and payment data
- f) Planning and control data
- g) information (from third parties, e.g. credit agencies, or from public directories)

h) data recorded by the client in the client's software

3. Technical-organizational measures

(1) The contractor shall document the implementation of the technical and organisational measures set out and required in advance of the award of the contract before the start of processing, in particular with regard to the concrete execution of the contract, and hand them over to the customer for inspection. If accepted by the client, the documented measures become the basis of the order. If the customer's inspection/audit reveals a need for adjustment, this must be implemented by mutual agreement.

(2) The contractor shall provide the security pursuant to Art. 28 para. 3 lit. c, 32 GDPR, in particular in connection with Art. 5 para. 1, para. 2 DS-GVO. Overall, the measures to be taken are measures of data security and to ensure a level of protection appropriate to the risk with regard to the confidentiality, integrity, availability and resilience of the systems. The state of the art, the implementation costs and the type, scope and purposes of processing as well as the different 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.

(3) The technical and organisational measures are subject to technical progress and further development. In this respect, the contractor is permitted to implement alternative adequate measures. The safety level of the defined measures must not be undershot. Significant changes must be documented.

4. Correction, restriction and deletion of data

(1) The contractor may not rectify, delete or restrict the processing of the data which are processed in the order on his own authority but only after the documented instructions of the principal. If a person concerned contacts the contractor directly in this regard, the contractor shall immediately forward this request to the customer.

(2) Insofar as the scope of services includes, the deletion concept, the right to oblivion, correction, data portability and information shall be ensured directly by the contractor in accordance with the documented instructions of the client.

5. Quality assurance and other obligations of the contractor

In addition to complying with the regulations of this order, the contractor has legal obligations according to Art. 28 to 33 GDPR; in this respect, in particular, he guarantees compliance with the following requirements:

- a) Written appointment of a data protection officer who performs his duties in accordance with Articles 38 and 39 of the GDPR. The contact details are easily accessible on the contractor's homepage. <https://www.caesar-data.de/impressum>
- b) The maintenance of confidentiality pursuant to Art. 28 para. 3 sentence 2 lit. b, 29, 32 para. 4 GDPR. In carrying out the work, the contractor shall only employ employees who are bound to confidentiality and who have been familiarised beforehand with the data protection provisions relevant to them. The contractor and any person subject to the contractor who has access to personal data may process such data exclusively in accordance with the instructions of the principal, including the powers granted in this contract, unless they are legally obliged to process them.

- c) The implementation and compliance with all technical and organisational measures required for this order in accordance with Art. 28 para. 3 sentence 2 lit. c, 32 GDPR[details in Annex 1].
- (d) On request, the contracting authority and the supplier shall cooperate with the supervisory authority in the performance of their tasks.
- e) Immediate information to the contracting authority on control actions and measures taken by the supervisory authority in so far as they relate to this mandate. This also applies if a competent authority investigates in the context of administrative or criminal proceedings with regard to the processing of personal data during order processing at the contractor.
- f) Insofar as the principal for his part is subject to an inspection by the supervisory authority, administrative or criminal proceedings, the liability claim of a person concerned or a third party or any other claim in connection with the processing of the order with the contractor, the contractor must support him to the best of his ability.
- (g) The contractor shall regularly monitor internal processes and technical and organisational measures to ensure that processing within his area of responsibility is carried out in accordance with the requirements of the applicable data protection legislation and that the rights of the data subject are protected.
- h) Verifiability of the technical and organisational measures taken vis-à-vis the customer within the scope of his control powers in accordance with Clause 7 of this contract.

6. Subcontracts

(1) Subcontracting relationships within the meaning of this provision shall be understood to mean those services which relate directly to the provision of the principal service. This does not include ancillary services which the contractor uses e.g. as telecommunication services, postal/transport services, maintenance and user services or the disposal of data carriers as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. However, in order to guarantee data protection and data security of the client's data, the contractor is obliged to take appropriate and legally compliant contractual agreements and control measures, even in the case of outsourced ancillary services.

(2) The contractor may only commission subcontractors (further contractors) with the prior express written or documented consent of the client. The Contractor shall specify all subcontracting relationships already existing at the time of the conclusion of the Contract in "Annex 1" to this Contract.

(3) The transfer of the client's personal data to the subcontractor and his first action are only permitted if all requirements for subcontracting are met.

(4) If the subcontractor performs the agreed service outside the EU/EEA, the contractor shall take appropriate measures to ensure the admissibility under data protection law. The same applies if service providers within the meaning of para. 1 sentence 2 are to be used.

7. Control rights of the client

- (1) The customer has the right to carry out inspections in consultation with the contractor or to have them carried out by inspectors to be appointed in individual cases. He has the right to satisfy himself of the contractor's compliance with this agreement in his business operations by means of spot checks, which as a rule must be notified in good time.
- (2) The contractor shall ensure that the contracting authority can satisfy itself of the contractor's compliance with the obligations pursuant to Art. 28 GDPR. The contractor undertakes to provide the customer with the necessary information on request and in particular to provide evidence of the implementation of the technical and organisational measures.
- (3) The proof of such measures, which do not only concern the concrete order, can take place via current testates, reports or report extracts of independent authorities (e.g. auditor, audit, data protection representative, IT-security department, data protection auditors, quality auditors);
4. In order to enable the contracting authority to carry out checks, the consultant may claim remuneration.

8. Notification in the event of breaches by the contractor

- (1) The contractor shall assist the contracting entity in complying with the obligations referred to in Articles 32 to 36 of the DS GMOs concerning the security of personal data, reporting obligations in the event of data leaks, data protection impact assessments and prior consultations. This includes, among other things
 - a) ensuring an adequate level of protection through technical and organisational measures which take into account the circumstances and purposes of the processing as well as the predicted probability and severity of a possible infringement of rights due to security gaps and enable an immediate determination of relevant infringement events
 - b) the obligation to report violations of personal data to the client without delay
 - c) the obligation to support the contracting authority in its duty to inform the party concerned and to make all relevant information available to him without delay in this connection
 - d) the support of the contracting entity for its data protection impact assessment
 - e) assisting the contracting entity in prior consultations with the supervisory authority
- (2) The contractor can claim compensation for support services that are not included in the service description or are not attributable to misconduct on the part of the contractor.

9. Remuneration

The remuneration of the contractor shall be agreed separately.

10. authority of the principal

- (1) The client confirms verbal instructions without delay (at least in text form).
- (2) The contractor shall inform the principal without delay if he is of the opinion that an instruction violates data protection regulations. The contractor is entitled to suspend the execution of the corresponding instruction until it is confirmed or changed by the customer.

11. Deletion and return of personal data

(1) Copies or duplicates of the data will not be made without the knowledge of the client. Excluded from this are backup copies, insofar as they are necessary to guarantee proper data processing, as well as data which are necessary with regard to compliance with legal storage obligations.

(2) After completion of the contractually agreed work or earlier upon request by the customer - at the latest upon termination of the service agreement - the contractor shall hand over to the customer all documents, processing and usage results created and data stocks in connection with the contractual relationship or destroy them in accordance with data protection regulations after prior consent. The same applies to test and scrap material. The deletion record must be submitted on request.

(3) Documentation that serves as proof of orderly and proper data processing shall be stored by the contractor after the end of the contract in accordance with the respective retention periods. He can hand them over to the client at the end of the contract.

11. Confidentiality obligations

(1) Both parties undertake to treat all information received in connection with the execution of this contract as confidential for an unlimited period of time and to use it only for the execution of the contract. Neither party is entitled to use this information in whole or in part for purposes other than those just mentioned or to make this information accessible to third parties.

(2) The above obligation does not apply to information which one of the parties has demonstrably received from third parties without being bound to secrecy or which is publicly known.

12. Safeguarding the rights of those concerned

(1) The client is solely responsible for the protection of the rights of the persons concerned.

(2) As far as a cooperation of the contractor is necessary for the protection of rights of the persons concerned - in particular for information, correction, blocking or deletion - by the customer, the contractor will take the necessary measures according to the instructions of the customer.

(3) This shall be without prejudice to any regulations regarding any remuneration of additional expenses arising from cooperation services in connection with assertion of rights of the parties concerned against the customer with the contractor.

Client

Contractor

Place, Date

Sonthofen, 09.05.2018

Place, Date

Stamp, signature

Stamp, signature



caesar data & software GmbH
Hindlangstr. 35 c-9 - 87327 Sonthofen
Tel.: 08321 / 8740-0 - Fax: 08321 / 8740 18
Info@Caesar-Data.de | www.caesar-data.de

Annex 1 – Subcontracts

For the processing of data on behalf of the principal, the contractor uses services of third parties who process data on his behalf ("subcontractors"). Changes or additions can be seen on our website and will be updated as required.

These are the following companies:

SoftTec Group GmbH

Hindelanger Straße 35

87527 Sonthofen

caesar data & software GmbH

Hindelanger Straße 35

87527 Sonthofen

Comtrance GmbH

In der Steele 35

40599 Düsseldorf

Annex 2 – Technical-organizational measures

1. To protect the confidentiality of personal data

- entrance control
No unauthorized access to data processing systems through spatially secured servers to which only authorized persons have access
- entrance control
No unauthorized system use, through secure passwords, automatic locking mechanisms, encryption of data carriers and use of suitable security software (virus protection, firewall)
- access control
Use of authorization concepts and demand-oriented access rights with corresponding password guidelines. Accesses are logged. Files are duly destroyed after expiry of the retention period.
- separation control
Data is stored separately on different servers according to the purpose of processing. Database rights are limited and appropriately granted and pseudonymised if required.

2. Maintaining the integrity of personal data

- Transfer control
No unauthorized reading, copying, modification or removal during electronic transmission or transport by encryption, Virtual Private Networks (VPN), electronic signature.
- input control
Determining whether and by whom personal data has been entered, changed or removed in data processing systems by logging access and assigning rights.

3. Maintaining the availability of personal data

- Availability control
Protection against accidental or deliberate destruction or loss through backup strategies, uninterruptible power supply (UPS), virus protection, firewall, reporting channels and emergency plans. Rapid recoverability in the event is ensured.
- order control
Contractors who process data on behalf of the client are carefully checked. AV contracts with contractors are concluded.

4. Procedures for regular review, evaluation and evaluation

Internal control of data security procedures, policies and concepts