

# Contract of the Order processing personal data according to Article 28 of the 3 DS-GVO

between

and

d.velop cloud **customer**

ecm:one GmbH  
Von-Vincke-Str. 5-7  
48143 Münster

*represented by*

Martin Odinius (CEO)

in the following: **Client**

in the following: contractor

## 1 Introduction, Scope, Definitions

- (1) This contract regulates the rights and obligations of the principal and the agent (hereinafter referred to as "parties") in the context of processing of personal data on behalf of the principal.
- (2) This Agreement shall apply to all activities in which employees of the Contractor or subcontractors (subcontractors) commissioned by the Contractor process personal data of the Client.
- (3) Terms used in this Treaty shall be understood in accordance with their definition in the EU Basic Regulation on data protection. In this sense, the contracting authority is the "responsible party" and the contractor the "processor". Insofar as declarations in the following are to be made "in writing", the written form according to § 126 BGB is meant. In all other respects, declarations may also be made in another form, provided that reasonable verifiability is ensured.

## 2 Subject and duration of processing

- (1) The object of the processing of personal data is the provision of the Cloud Services designated in the main contract, including the associated maintenance, care and support services by the Contractor for the Customer. Insofar as agreed in the main contract, this also includes the prior migration of data from an existing system at the Customer to the Cloud Services provided by the Contractor.
- (2) The duration of processing is specified in the main contract.

## 3 Type and purpose of data collection, -processing or -use:

### 3.1 Type and purpose of the processing

Type of processing (according to the definition in Art. 4 No. 2 DS-GVO):

Organisation, ordering, storage, adaptation or modification, reading and querying

Purpose of the processing

Services within the scope of the service contract, such as telephone assistance, remote/remote maintenance services, e.g. error documentation, tracing of document recognition results based on master data

### 3.2 Type of data

The following data are processed:

- First and last name
- Contact details
- Tax information (UstId, tax number)
- Bank details

#### 3.2.1 Categories of data subjects

The persons concerned by the processing operation are:

- Customers
- Suppliers
- Employees

## 4 Duties of the Contractor

- (1) The Contractor shall process personal data exclusively as contractually agreed or as instructed by the Client, unless the Contractor is legally obligated to a specific processing. If such obligations exist for him, the Contractor shall inform the Customer of these obligations prior to processing, unless the Contractor is prohibited by law from doing so. Furthermore, the contractor shall not use the data provided for processing for any other purposes, in particular not for his own purposes.
- (2) The contractor confirms that he is aware of the relevant general data protection regulations. He observes the principles of proper data processing.
- (3) The contractor undertakes to maintain strict confidentiality during processing.
- (4) Persons who may gain knowledge of the data processed in the order must undertake in writing to maintain confidentiality, unless they are already legally subject to a relevant confidentiality obligation.
- (5) The Contractor warrants that the persons employed by it for processing have been made familiar with the relevant provisions of data protection and this Agreement prior to the start of the processing. Appropriate training and awareness-raising measures shall be repeated at appropriate intervals. Contractor shall ensure that persons employed for processing orders are appropriately instructed and monitored on an ongoing basis with regard to compliance with the data protection requirements.
- (6) In connection with the commissioned processing, the contractor shall assist the contracting party in drawing up and updating the list of processing activities and in carrying out the data protection impact assessment. All necessary information and documentation shall be kept available and shall be provided to the Customer immediately upon request.
- (7) If the customer is subject to an inspection by supervisory authorities or other bodies or if affected persons assert rights against him, the contractor undertakes to support the customer to the extent necessary insofar as the processing in the order is affected.
- (8) The Contractor may only provide information to third parties or the person concerned with the prior consent of the Client. He will immediately forward inquiries addressed directly to him to the customer.
- (9) Insofar as legally obliged, the contractor shall appoint a competent and reliable person as data protection officer. It must be ensured that there are no conflicts of interest for the data protection officer. In cases of doubt, the client may contact the data protection officer directly. The Contractor shall inform the Client immediately of the contact details of the Data Protection Officer or give reasons why no Data Protection Officer has been appointed. The Contractor shall inform the Client immediately of any changes in the person or the internal tasks of the Data Protection Officer.
- (10) The processing of orders is generally carried out within the EU or the EEA. Any relocation to a third country may only take place with the express consent of the client and under the conditions contained in Chapter V of the Basic Data Protection Regulation and in compliance with the provisions of this contract.
- (11) If the contractor is not established in the European Union, he shall appoint a responsible contact person in the European Union in accordance with Article 27 of the Basic Data Protection Regulation. The contact data of the contact person as well as all changes in the person of the contact person must be communicated to the client without delay.

## 5 Technical and organisational measures

- (1) The data security measures described in Annex 1 are defined as mandatory. They define the minimum owed by the contractor. The description of the measures must be so detailed that a competent third party can at all times determine beyond doubt what the owed minimum is to be on the basis of the description alone. No reference may be made to information which cannot be directly taken from this agreement or its annexes.
- (2) The data security measures can be adapted to technical and organizational developments as long as the level agreed upon here is not undercut. The Contractor shall implement any changes required to maintain information security without delay. The Customer must be informed of any changes without delay. Significant changes are to be agreed between the parties.
- (3) If the security measures taken do not or no longer meet the requirements of the Customer, the Contractor shall notify the Customer immediately.
- (4) The contractor assures that the data processed in the order is strictly separated from other data stocks.
- (5) Copies or duplicates will not be made without the knowledge of the customer. This does not apply to technically necessary, temporary copies, provided that an impairment of the data protection level agreed here is excluded.
- (6) The processing of data in private homes is only permitted with the prior written consent of the client in individual cases. Insofar as such processing is carried out, the Contractor shall ensure that a level of data protection and data security corresponding to this contract is maintained and that the control rights of the Customer specified in this contract can also be exercised without restriction in the private apartments concerned. The processing of data by order with private devices is permitted under no circumstances.
- (7) Dedicated data carriers which originate from the client or are used for the client are specially marked and are subject to ongoing administration. They must be stored appropriately at all times and must not be accessible to unauthorised persons. Entrances and exits shall be documented.
- (8) The client can check the fulfilment of the contractor's obligations at any time by agreement.

## 6 Rules for the correction, deletion and blocking of data

- (1) The Contractor shall only correct, delete or block data processed within the scope of the order in accordance with the contractual agreement reached or as instructed by the Client.
- (2) The contractor shall comply with the corresponding instructions of the customer at any time and also beyond the termination of this contract.

## 7 Subcontracting relations

- (1) The commissioning of subcontractors is only permitted with the written consent of the customer in individual cases.
- (2) Consent shall only be possible if the subcontractor has been contractually assigned at least data protection obligations comparable to those agreed in this contract. On request, the Client shall be given access to the relevant contracts between the Contractor and the subcontractor.
- (3) It must also be possible for the customer's rights to be effectively exercised against the subcontractor. In particular, the customer must be entitled to carry out checks at any time to the extent specified here, including on subcontractors, or to have them carried out by third parties.

- (4) The responsibilities of the contractor and the subcontractor shall be clearly demarcated.
- (5) Further subcontracting by the subcontractor is not permitted.
- (6) The Contractor shall carefully select the subcontractor with special consideration of the suitability of the technical and organisational measures taken by the subcontractor..
- (7) The forwarding of data processed in the order to the subcontractor shall only be permitted after the contractor has satisfied himself in a documented manner that the subcontractor has fulfilled his obligations in full. The Contractor shall submit the documentation to the Client without being requested to do so.
- (8) The use of subcontractors who provide processing services on behalf of a third party not exclusively from the territory of the EU or EEA is only possible if the conditions set out in Chapter 4 (10) and (11) of this agreement are respected. In particular, it is only permissible to the extent and for as long as the subcontractor provides adequate data protection guarantees. The Contractor shall inform the Principal of the specific data protection guarantees offered by the Subcontractor and how proof thereof can be obtained.
- (9) The Contractor shall carry out appropriate checks on compliance with the subcontractor's obligations regularly, at the latest every 12 months. The inspection and its results shall be documented in such a meaningful manner that they are comprehensible to a competent third party. The documentation must be presented to the client without being asked.
- (10) If the subcontractor does not comply with his data protection obligations, the contractor shall be liable to the customer for this.
- (11) At present, the subcontractors listed in Appendix 2 with their names, addresses and order contents are engaged in the processing of personal data to the extent specified therein and approved by the customer. The Contractor's other obligations towards subcontractors set out in this Appendix shall remain unaffected.
- (12) Subcontracting relationships within the meaning of this contract are only those services which have a direct connection with the provision of the main service. Ancillary services such as transport, maintenance and cleaning as well as the use of telecommunications services or user services are not covered. The Contractor's obligation to ensure compliance with data protection and data security in these cases as well remains unaffected.

## 8 Rights and duties of the client

- (1) The client alone is responsible for assessing the permissibility of the commissioned processing and for safeguarding the rights of data subjects.
- (2) The client shall issue all orders, partial orders or instructions in a documented manner. In urgent cases, instructions may be given verbally. The client will confirm such instructions in a documented form without delay.
- (3) The Client shall inform the Contractor immediately if he discovers errors or irregularities in the examination of the order results.
- (4) The customer is entitled to check compliance with the regulations on data protection and the contractual agreements at the contractor's premises to a reasonable extent, either himself or through third parties, in particular by obtaining information and inspecting the stored data and the data processing programs as well as other on-site inspections. The persons entrusted with the control shall be granted access and insight by the contractor to the extent required. The Contractor is obliged to provide the necessary information, demonstrate procedures and keep records that are necessary to carry out a check.

- (5) Checks at the contractor's premises shall be carried out without causing any avoidable disruption to his business operations. Unless otherwise indicated for urgent reasons to be documented by the Customer, inspections shall be carried out after reasonable advance notice and during the business hours of the Contractor and not more frequently than every 12 months. As far as the Contractor provides evidence of the correct implementation of the agreed data protection obligations as provided for in Chapter 5 (8) of this Agreement, an inspection shall be limited to random checks.

## 9 Duty of notification

- (1) The Contractor shall notify the Client without delay of violations of the protection of personal data. Reasonable suspicions of such violations must also be communicated. The notification must be sent to an address specified by the Customer at the latest within 24 hours of the Contractor becoming aware of the relevant event. It must contain at least the following information:
  - a. a description of the nature of the breach of personal data protection, indicating, where possible, the categories and approximate number of data subjects, the categories and approximate number of personal data sets concerned;
  - b. the name and contact details of the Data Protection Officer or any other contact point for further information;
  - c. a description of the probable consequences of the violation of personal data protection;
  - d. a description of the measures taken or proposed by the contractor to remedy the breach of personal data protection and, where appropriate, measures to mitigate its possible adverse effects
- (2) Also to be reported immediately are significant disruptions in the execution of the order as well as violations of the contractor or the persons employed by him against data protection regulations or the stipulations made in this contract.
- (3) The Contractor shall inform the Client without delay of inspections or measures by supervisory authorities or other third parties, insofar as these have any connection with the processing of the order.
- (4) The Contractor warrants to support the Client to the necessary extent in fulfilling the Client's obligations under Articles 33 and 34 of the Basic Regulation on Data Protection.

## 10 Instructions

- (1) The customer reserves a comprehensive right of instruction regarding the processing in the order.
- (2) Client and contractor shall name the persons exclusively authorised to issue and accept instructions in Annex 3.
- (3) In the event of a change or long-term inability of the designated persons, successors or representatives must be notified to the other party without delay.
- (4) The Contractor shall immediately inform the Client if, in his opinion, an instruction issued by the Client violates statutory provisions. The Contractor is entitled to suspend the execution of the corresponding instruction until it is confirmed or amended by the person responsible at the Client.
- (5) The contractor shall document instructions given to him and their implementation.

## 11 Termination of the contract

- (1) Upon termination of the contractual relationship or at any time at the request of the Client, the Contractor shall, at the Client's discretion, either destroy the data processed in the order or hand

them over to the Client. All existing copies of the data must also be destroyed. Destruction must be carried out in such a way that it is no longer possible to restore even residual information with reasonable effort. Physical destruction shall be carried out in accordance with DIN 66399, whereby at least protection class 1 shall apply.

- (2) The Contractor shall be obliged to bring about the immediate return or deletion also in the case of subcontractors.
- (3) The contractor must provide proof of proper destruction and submit it to the customer without delay.
- (4) Documentation which serves as proof of proper data processing shall be kept by the Contractor in accordance with the respective retention periods even beyond the end of the contract. He can hand them over to the customer at the end of the contract for his own relief.

## 12 Payment

The payment of the contractor is finally regulated in the main contract. There shall be no separate remuneration or reimbursement of costs within the scope of this contract.

## 13 Liability

- (1) The Client and Contractor shall be jointly and severally liable for compensation for damages suffered by a person due to inadmissible or incorrect data processing within the scope of the contractual relationship.
- (2) The Contractor shall bear the burden of proof that any damage is not the result of a circumstance for which he is responsible, insofar as the relevant data were processed by him under this agreement. As long as this proof has not been provided, the contractor shall indemnify the customer on first demand from all claims made against the customer in connection with the processing of the order. Under these conditions, the Contractor shall also reimburse the Customer for all legal defense costs incurred.
- (3) The Contractor shall be liable to the Client for any damage culpably caused by the Contractor, its employees or its agents or subcontractors employed by the Contractor in connection with the performance of the commissioned contractual service.
- (4) Points (2) and (3) shall not apply insofar as the damage is caused by the correct implementation of the commissioned service or an instruction issued by the client.

## 14 Contractual penalty

- (1) In case of violation of the agreements of this contract, a no-fault contractual penalty of € 500,- per individual case is agreed. The contractual penalty shall be forfeited in particular in the event of deficiencies in the implementation of the agreed technical and organisational measures. In the case of permanent violations, each calendar month in which the violation occurs in whole or in part shall be considered an individual case. The plea of continuation is excluded.
- (2) The contractual penalty has no influence on other claims of the client.

## 15 Special right of termination

- (1) The Customer may terminate the main contract and this Agreement at any time without notice ("extraordinary termination") if there is a serious breach by the Contractor of data protection regulations or the provisions of this Agreement, if the Contractor is unable or unwilling to carry out

a lawful instruction of the Customer or if the Contractor refuses control rights of the Customer in breach of contract.

- (2) A serious breach shall be deemed to have occurred in particular if the contractor fails or has failed to perform to a significant extent the obligations set out in this agreement, in particular the agreed technical and organisational measures.
- (3) In the case of minor infringements, the Customer shall set the Contractor a reasonable period of time to remedy the situation. If the remedy does not take place in time, the customer is entitled to extraordinary termination as described in this section.
- (4) The Contractor shall reimburse the Client for all costs incurred by the Client due to the premature termination of the main contract or this contract as a result of an extraordinary termination by the Client.

## 16 Others

- (1) Both parties are obligated to treat confidentially all knowledge of business secrets and data security measures of the other party obtained within the scope of the contractual relationship, even after the termination of the contract. If there is any doubt as to whether any information is subject to the obligation of secrecy, it shall be treated as confidential until the other party releases it in writing.
- (2) If the property of the Customer at the Contractor is endangered by measures of third parties (such as seizure or confiscation), by insolvency or composition proceedings or by other events, the Contractor shall notify the Customer immediately.
- (3) The written form is required for collateral agreements.
- (4) The plea of the right of retention within the meaning of § 273 BGB is excluded with regard to the data processed in the order and the associated data carriers.
- (5) Should individual parts of this agreement be ineffective, this shall not affect the effectiveness of the rest of the agreement.

# Annex 1 – Technical and organisational measures

In the following, the technical and organizational measures for ensuring data protection and data security are defined, which the contractor must at least set up and continuously maintain. The aim is to guarantee in particular the confidentiality, integrity and availability of the information processed in the order.

## 1 Confidentiality (Art. 32 Abs. 1 lit. b DS-GVO)

<p>Access control</p> <p>No unauthorised access to data processing equipment,</p>	<p>Office:</p> <ul style="list-style-type: none"> <li>- Key / key allocation (documented allocation)</li> <li>- Door security (electric door openers etc.)</li> <li>- Authorization for elevator</li> </ul>
<p>Access control</p> <p>No unauthorized system use</p>	<ul style="list-style-type: none"> <li>- Active Directory</li> <li>- Password procedures (including special characters, minimum length, regular change of the complex password)</li> <li>- Automatic locking of the screen (e.g. password or pause)</li> <li>- Setup of a user master record per user</li> <li>- Use of Anti-Mailware Software</li> <li>- Use of Firewall</li> </ul>
<p>Access control</p> <p>No unauthorized reading, copying, modification or removal within the system</p>	<p>Appropriate setup of the authorization concept and access rights and their monitoring and logging:</p> <ul style="list-style-type: none"> <li>- Differentiated authorizations (profiles, roles, groups) <ul style="list-style-type: none"> <li>o File system</li> <li>o Applications</li> </ul> </li> <li>- Controlled remote access <ul style="list-style-type: none"> <li>o Through firewall and VPN rules</li> </ul> </li> <li>- Maintenance guidelines</li> </ul>
<p>Trennungskontrolle</p> <p>Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden</p>	<ul style="list-style-type: none"> <li>- Earmarking of data / client processing</li> <li>- separation of functions (production / test)</li> <li>- Data from different clients are stored separately</li> </ul>
<p>Pseudonymisation</p> <p>Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;</p>	<p>Pseudonymisation is not used in the company.</p>

(Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

## 2 Integrity (Art. 32 Abs. 1 lit. b DS-GVO)

<p>Passing on control</p> <p>No unauthorized reading, copying, modification or removal during electronic transmission or transport</p>	<p>measures relating to transport, transfer and transmission or storage on data media (manual or electronic) and subsequent verification:</p> <ul style="list-style-type: none"><li>- Encryption techniques / tunnel connection (VPN)</li><li>- Encrypted mail transport</li></ul>
<p>Input control</p> <p>Determining whether and by whom personal data have been entered, changed or removed from data processing systems</p>	<p>measures for subsequent verification whether data have been entered, modified or removed (deleted) and by whom:</p> <ul style="list-style-type: none"><li>- Logging</li><li>- User identification</li></ul>

## 3 Availability and resilience (Art. 32 Abs. 1 lit. b DS-GVO)

<p>Availability control</p>	<p>Measures for data backup (physical / logical):</p> <ul style="list-style-type: none"><li>- Backup procedure (multi-level backup system)</li><li>- Overvoltage protection</li><li>- Storage Backups in a Private Cloud</li><li>- - Virus protection / Firewall</li><li>- Fire protection measures<ul style="list-style-type: none"><li>o Fire alarm system</li></ul></li><li>- Use of anti-malware software and firewall</li></ul>
<p>Rapid recoverability</p> <p>(Art. 32 Abs. 1 lit. c DS-GVO)</p>	<p>Ensuring complete, consistent backups - Acronis TrueImage</p> <p>Backup of the hard disks as complete images - byte exact -</p>

## 4 Procedures for periodic review, assessment and evaluation (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Incident-Response-Management	Reporting process by type. 33, 34 (DS-GVO)
Privacy Friendly Presets (Art. 25 Abs. 2 DS-GVO)	<ul style="list-style-type: none"><li>- SMTP-Server (STARTTLS)</li><li>- https</li><li>- VPN-accesses</li></ul>
Order Control	Measures (technical / organisational) to demarcate the competences between client and sub-contractor: <ul style="list-style-type: none"><li>- Clear contract design with sub-contractors on the basis of the main contract with the client</li><li>- Contract for commissioned data processing with service providers under Art. 28 DS-GVO</li><li>- Formalised placing of orders through order forms and contracts</li><li>- Control of the execution of the contract</li></ul>

## Anlage 2 – Data protection officer

No data protection officer was appointed at the contractor because the contractor's company size is currently in the order of magnitude of a micro-enterprise.