General Terms and Conditions of A1 Digital Deutschland GmbH for processing of personal data on behalf of customers (GTC DPA)

V2.0, Applicable from July 2023
Autor: A1 Digital Deutschland Data Privacy Officer

1. Scope, subject matter and duration of the order

(1) These GTC DPA form the contractual basis for existing and future contractual relationships between A1 Digital Deutschland GmbH („A1 Digital") and customers of A1 Digital, insofar as A1 Digital processes personal data on behalf of the customer (hereinafter also referred to as "controller") as processor pursuant to Art. 28 EU-GDPR; the GTC DPA apply in particular to all data center-, application- and support services provided by A1 Digital, insofar as personal data of customers of A1 Digital are processed in this context.

(2) The object of the order results from the respective contractual relationship (hereinafter referred to as "service agreement"), which is the legal basis for the performance of data processing by the processor.

(3) The duration of this order (term) corresponds to the term of the respective service agreement.

2. Description of data processing

(1) The nature and purpose of the processing, the categories of data subjects and the type of personal data are specifically described in the respective service agreement including the appendix on data protection.

(2) The contractually agreed data processing may only be provided by transfer to a third country if the special requirements of Art. 44 et seq. GDPR are fulfilled. The adequate level of protection in this third country is either

a) established by an adequacy decision of the Commission (Art. 45 para. 3. GDPR); or
b) is ensured by binding corporate rules (Art. 46 para. 2 no. b in conjunction with 47 GDPR); or
c) is ensured by standard data protection clauses (Art. 46 para. 2 no. c and d GDPR); or
d) is ensured in accordance with approved codes of conduct (Art. 46 para. 2 no. e in conjunction with 40 GDPR); or
e) is ensured by an approved certification mechanism (Art. 46 para. 2 no. f in conjunction with 42 GDPR); or
f) is ensured by other measures (Art. 46 para. 2 lit. a, para. 3 no. a and b GDPR).

If none of these requirements are met, data processing in the third country is not permitted.

3. Technical-Organisational Measures

(1) The processor shall document the implementation of the technical and organisational measures set out and required prior to the order and the beginning of data processing, in particular with regard to the actual execution of the order.

(2) The processor shall provide security in accordance with Art. 28 para. 3 no. c, 32 GDPR, in particular in conjunction with Art. 5 para. 1, para. 2 GDPR. Overall, the measures to be taken are measures for 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.
In doing so, the state of the art, the costs of implementation and the nature, scope and purpose of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons within the meaning of Art. 32 para. 1 GDPR shall be taken into account. Unless otherwise specified in the service agreement, it shall be the responsibility of the processor to ensure the appropriate level of protection for the processing, in particular by a combination of the technical and organisational measures specified in the Annex. The processor shall be permitted to implement alternative adequate measures. The security level of the specified measures may not be undercut.

4. Rectification, Restriction and Erasure of Data

(1) The processor may rectify, erase (delete) or restrict the processing of data processed on behalf only in accordance with the documented instructions from the controller. If a data subject contacts the processor directly in this regard, the processor shall immediately forward this request to the controller.

(2) Insofar as the scope of services includes, a deletion concept, the right of access, the right to erasure (right to be forgotten), right to rectification and data portability in accordance with the documented instructions of the person responsible shall be ensured directly by the processor.

5. Quality Assurance and other Obligations of the Processor

In addition to compliance with the provisions of this order, the processor shall have legal obligations pursuant to Articles 28 to 33 GDPR; to this extent the processor shall in particular ensure compliance with the following requirements:

a) The written appointment of a data protection officer who performs his duties in accordance with Articles 38 and 39 GDPR. The contact details of the data protection officer will be communicated to the controller for the purpose of direct contact. The controller will be informed immediately of any change of the data protection officer.
b) The maintenance of confidentiality pursuant to Art. 28 para. 3 sentence 2 no. b, 29, 32 para. 4 GDPR. The processor shall ensure that persons authorised to process the personal data have committed themselves to confidentiality and have been familiarised beforehand with the data protection provisions relevant to them. The processor and any person subordinated to the processor who has access to personal data may only process these data in accordance with the service agreement or the instructions of the controller, unless they are legally obliged to process them.
c) The implementation of and compliance with all technical and organisational measures required for this order pursuant to Art. 28 para. 3 sentence 2 no. c, 32 GDPR.

d) Upon request, the controller and the processor shall cooperate with the supervisory authority in the performance of their duties.
e) To the extent permitted by law, to inform the controller without delay of control actions and measures taken by the supervisory authority insofar as they relate to this order. In this case, the processor shall refer the authority to the controller.
f) Insofar as the controller is subject to a supervisory authority inspection, an administrative offence or criminal procedure, the liability claim of a data subject or a third party or any other claim in connection with the data processing, the processor shall support the controller to the best of his ability.
(g) The processor shall regularly monitor internal processes and technical and organisational measures to ensure that processing within his sphere of responsibility is carried out in accordance with the requirements of applicable data protection law and that the protection of the rights of data subjects is ensured.
h) The verifiability of the technical and organisational measures taken vis-à-vis the controller within the scope of the controller's audit rights in accordance with section 7 of this contract.

6. Subcontracting

(1) For the purposes of this provision, subcontracting shall mean services which relate directly to the provision of the main service. This does not include ancillary services used by the processor e.g. as telecommunications services, postal/transport services, maintenance and support 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 the data security of the data of the controller, the processor is obliged to make appropriate contractual agreements and audit measures in accordance with the law, even in the case of outsourced ancillary services.

(2) Insofar as not already stipulated in the service agreement, the processor may make use of further subcontractors (authorized persons) to support data processing in accordance with this agreement. It is agreed that the subcontractors used at the time the service agreement is concluded shall be deemed to be approved subcontractors. The processor shall inform the controller in writing of any change of subcontractor in sufficient time for the controller to be able to prohibit such a change of subcontractor, if necessary for objective reasons. If an affiliated company is used as a subcontractor, the consent of the controller shall be deemed to have been given.

(3) All subcontractors shall be subject to the same obligations as the processor under this agreement or agreements related to this agreement.

(4) The processor shall at all times be liable to the controller for compliance with this agreement and related agreements by the sub-contractors.

7. Right to Audit

(1) The processor shall ensure that the controller can verify that the processor's obligations under Art. 28 GDPR have been complied with. The processor undertakes to provide the controller with the necessary information upon request and, in particular, to prove that the technical and organisational measures have been implemented.

(2) Evidence of such measures, which do not only concern the specific order, may be provided by:

a) Compliance with approved codes of conduct pursuant to Art. 40 GDPR;
b) Certification in accordance with an approved certification procedure pursuant to Art.
c) 42 GDPR;
d) Current attestations, reports or extracts of reports from independent bodies (e.g. auditors, data protection officers, IT security department, data protection auditors, quality auditors);
e) An appropriate certification by IT security or data protection audit (e.g. according to basic protection BSI or ISO/IEC); e) Annual reports by the processor.

(3) If further information is required by the controller in order to fulfil his own audit obligations or if the competent authority has issued a corresponding order, the controller shall inform the processor in writing so that the processor can provide this information or grant the controller access to the information.

(4) If the above information is not deemed sufficient to fulfil the audit obligation under the applicable law, or if a material breach of data protection has occurred for which the processor is responsible, the controller shall have the right, in coordination with the processor, to carry out verifications or have them carried out by auditors to be appointed in each individual case. The processor shall have the right to verify compliance with this agreement by the processor in the processor's business by carrying out spot checks to be notified one month in advance.

(5) In order to carry out an inspection, the controller shall send a detailed audit/control plan to the processor at least two weeks before the scheduled inspection date, stating the scope, duration and start date of the inspection. The processor shall review the audit/control plan and communicate to the controller any significant concerns and questions, such as requests for information, that may affect the processor's security, privacy or employment policy. In all cases, the processor shall cooperate with the controller to agree a final audit/control plan.

(6) The audit shall take place during regular business hours, in accordance with the operating policies of the processor's facility, and shall not unduly interfere with the processor's operations. The processor shall make reasonable efforts to provide the auditor with the requested information.

(7) The controller shall bear the cost of carrying out the controls himself. The processor may assert a claim for remuneration for further support services. For this purpose, the processor shall submit an offer which shall be mutually agreed.

8. Assistance

(1) The processor shall assist the controller in complying with the obligations set out in Articles 32 to 36 GDPR, regarding personal data security obligations, reporting obligations in the event of data breaches, data protection impact assessments and prior consultations. These include, but are not limited to:

a) ensuring an adequate level of protection through technical and organisational measures that take into account the circumstances and purposes of the processing as well as the predicted likelihood and severity of a possible breach of rights through security gaps and enable an immediate identification of relevant breach events;

b) the obligation to report personal data breaches to the controller without undue delay;
c) the obligation to assist the controller with regard to his duty to provide information to the data subject and, in this context, to make all relevant information available to the controller without undue delay;
d) assist the controller in carrying out his data protection impact assessment;
e) assisting the controller in prior consultations with the supervisory authority.

(2) For support services which are not included in the description of services or which are not attributable to misconduct on the part of the processor, the processor may claim remuneration to be agreed by mutual agreement.

9. Instructions

(1) In addition to the contractually agreed specifications, written instructions may also be issued by the controller by e-mail (in text form).

(2) The processor shall immediately inform the controller if the processor is of the opinion that an instruction violates data protection regulations. The processor shall be entitled to suspend the execution of the corresponding instruction until it has been confirmed or amended by the controller.

10. Deletion and Return of Personal Data

(1) Copies or duplicates of the data shall not be made without the knowledge of the controller. Excepted from this are backup copies insofar as they are necessary to ensure proper data processing, as well as data which are necessary with regard to compliance with statutory storage obligations.

(2) Upon completion of the contractually agreed work or earlier upon request by the controller - at the latest upon termination of the service agreement - the processor shall hand over to the controller all documents in his possession, processing and usage results as well as data stocks created in connection with the contractual relationship and destroy them in accordance with data protection regulations. The same applies to test and scrap material. The deletion protocol must be submitted upon request.

(3) Documentations which serve as proof of the orderly and proper data processing shall be kept by the processor beyond the end of the contract in accordance with the respective retention periods. The processor may hand over the documentations to the controller at the end of the contract in order to relieve himself.

11. Governing Law and Jurisdiction

This agreement shall be exclusively subject to German law excluding its conflict of laws principles. Moreover, the place of jurisdiction shall be the Regional Court I, Munich.

Annex – Technical-Organisational Measures

1. Confidentiality (Art. 32 para. 1 no. b GDPR)

- Access control (physical security)
  No unauthorised access to data processing systems, e.g: magnetic or chip cards, keys, electric door openers, factory security or gatekeepers, alarm systems, video systems;
- Access control
  No unauthorised system use, e.g: (secure) passwords, automatic locking mechanisms, two-factor authentication, encryption of data media;
- Data access control
  No unauthorised reading, copying, modifying or removing within the system, e.g: Authorisation concepts and demand-oriented access rights, logging of accesses;
- Separation control
  Separate processing of data collected for different purposes, e.g. multi-client capability, sandboxing;
- Pseudonymisation (Art. 32 para. 1 no. a GDPR; Art. 25 para. 1 GDPR) The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without additional information, provided that such additional information is kept separately and is subject to appropriate technical and organisational measures.

2. Integrity (Art. 32 para. 1 no. b GDPR)

- Transfer control
  No unauthorised reading, copying, modification or removal during electronic transmission or transport, e.g.: encryption, Virtual Private Networks (VPN), electronic signature;
- Input control
  Determining whether and by whom personal data have been entered, altered or removed in data processing systems, e.g: logging, document management.

3. Availability and resilience (Art. 32 para. 1 no. b GDPR)

- Availability control
  Protection against accidental or deliberate 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;
- The ability to restore the availability in a timely manner (Art. 32 para. 1 no. c GDPR).

4. Process for regularly testing, assessing and evaluating (Art. 32 para. 1 no. d GDPR; Art. 25 para. 1 GDPR)

- Data Protection Management;
- Incident-Response Management;
- Data protection-friendly default settings (Art. 25 para. 2 GDPR).