[This template is shared publicly on https://www.iubenda.com/en/help/7680-data-processing-agreement-template-gdpr]

DPA model - English

Data Processing Agreement (DPA)

pursuant to art. 28 General Data Protection Regulation (GDPR)

between
.....

- the Controller –

.....

- the Processor -

[if applicable: Authorised Representative as of art. 27 GDPR:

.....]

1. Subject matter, term, personal data processed

(1) Subject matter

- The subject matter of the DPA and the thereto related processing activities result from the main contract signed by the parties on (DATE).

[*or*

- The Processor shall carry out the following processing activities:
  .....
  .....
  .....
  .....
  .....]

(2) Term

- The term of this DPA corresponds to the term of the main contract.

[*alternatively:* specify term]

(3) Categories of personal data

- The categories of personal data processed are:

- key personal data
- contact data
- key contract data
- customer history
- billing, invoicing and payment data
- other:..... [*please specify*]

(4) Categories of Data Subjects

- The personal data collected and processed related to:
  - customers
  - potential customers
  - subscribers
  - employees, collaborators
  - processors
  - authorised agents
  - reference persons
  - other:..... [*please specify*]

2. Processing within the EU and EEA

Data processing activities under this DPA shall only be performed within the European Union (EU) or the European Economic Area (EEA). Each and every transfer of data to a third country not part to the EU or EEA requires the prior agreement in writing by the Controller and shall only be carried out at the specific conditions set forth by Article 44 et seq. GDPR.

Notwithstanding the above, the Controller acknowledges and accepts by signature of this DPA that the processing of personal data shall also be carried out in the following countries pursuant to the following legal basis for transfer:

	A	B
1	**country**	**legal basis for transfer**
2	*e.g. Switzerland*	*e.g. adequacy decision*
3		
4		
5		
6		

Possible legal bases for transfer pursuant to the GDPR include:

- an adequacy decision issued by the European Commission (Article 45 Paragraph 3 GDPR);
- binding corporate rules (Article 46 Paragraph 2 Point b in conjunction with Article 47 GDPR);

- Standard Data Protection Clauses (Article 46 Paragraph 2 Points c and d GDPR);
- Codes of Conduct (Article 46 Paragraph 2 Point e in conjunction with Article 40 GDPR);
- Certification Mechanism. (Article 46 Paragraph 2 Point f in conjunction with Article 42 GDPR).
- other means:..... (Article 46 Paragraph 2 Point a, Paragraph 3 Points a and b GDPR)

3. Technical and Organisational Measures

(1) Prior to the execution of this DPA, the Processor shall demonstrate that all necessary technical and organizational measures, specifically with regard to the detailed performance of this DPA, have been adopted and shall, upon request, provide documented evidence thereof to the Controller. Upon acceptance by the Controller, such documented measures become binding part of this DPA and are attached to it. Insofar as an inspection/audit by the Controller shows the necessity for amendments, such amendments shall be implemented by mutual agreement.

(2) The Processor shall guarantee security in accordance with Article 28 Paragraph 3 Point c, and Article 32 GDPR in particular in conjunction with Article 5 Paragraph 1, and Paragraph 2 GDPR. Such measures shall guarantee data security and a protection level appropriate to the risk concerning confidentiality, integrity, availability, and resilience of the systems. The state of the art, implementation costs, the nature, scope and purposes of processing as well as the likelihood of data breaches and the severity of risks to the rights and freedoms of natural persons possibly resulting thereof within the meaning of Article 32 Paragraph 1 GDPR must be taken into account.

(3) The technical and organizational measures are subject to technical and technological progress and development. Hence, the Processor may adopt alternative adequate measures adapted to the changed technological environment. When doing so, the processing security level may not be reduced. Substantial changes must be documented.

4. Rectification, restriction and erasure of data

(1) The Processor may not rectify, erase or restrict the processing of data that is being processed on the Controller's behalf at its own initiative but only upon documented instructions by the Controller.

(2) Should a Data Subject contact the Processor directly concerning a rectification, erasure, or restriction of processing, the Processor shall immediately forward such Data Subject’s request to the Controller. The requests of erasure, rectification, data

portability and access shall be fulfilled by the Processor in accordance with documented instructions by the Controller without undue delay.

5. Quality assurance and other duties of the Processor

In addition to complying with the provisions of this DPA, the Processor commits to meet all applicable statutory requirements set forth at Articles 28 to 33 GDPR. Therefore, the Processor ensures, in particular, compliance with the following requirements:

- **Appointment of a Data Protection Officer (DPO)**
  The current DPO is:
  (FULL CONTACT DETAILS)**.....**
  .....
  .....
  The Processor shall inform the Controller without delay about any changes of Data Protection Officer.

  [*or*
  The Processor is not required to appoint a Data Protection Officer. Mr/Ms [enter: given name, surname, organizational unit, telephone, e-mail] is designated as the Contact Person on behalf of the Processor.]

- [→ pick only if applicable] **Appointment of a Representative**
  Since the Processor is established outside the EU & EEA it designates
  (FULL CONTACT DETAILS).....
  .....
  .....
  as Representative within the Union pursuant to Article 27 Paragraph 1 GDPR.

- **Confidentiality**
  Processing activities under this DPA shall only be performed by such employees or collaborators and agents that have been instructed by the Processor about the appropriate dealing with personal data and have been contractually subjected to confidentiality pursuant to art. 28 par. 3 (b) and art. 32 GDPR. The Processor and any person acting under its authority who has access to personal data, shall not process that data unless upon instructions by the Controller, including the powers granted under this DPA, unless they are required to do so by statutory law.
- **Technical and Organizational Measures**
  Implementation of and compliance with all appropriate Technical and Organizational Measures in the framework of this DPA, in particular as set forth at art. 32 GDPR. The Processor shall periodically monitor

the internal processes and the technical and organizational measures o ensure that processing within its area of responsibility is in accordance with the requirements of applicable data protection law and the protection of data subjects' rights. The Processor shall grant verifiability of the technical and organizational measures to the Controller as part of the Controller's supervisory powers referred to in sec. 7 of this contract.

- **Cooperation with Supervisory Authorities**
  The Controller and the Processor shall cooperate, on request, with the supervisory authority. The Controller shall be informed immediately of any inspections and measures executed by the supervisory authority, insofar as they relate to the activities under this DPA. This also applies insofar as the Processor is under investigation or is party to an investigation by a competent authority in connection with infringements to any provision regarding the processing of personal data in connection with the processing of this DPA. Insofar as the Controller is subject to an inspection by the supervisory authority, an administrative fine, a preliminary injunction or criminal procedure, a liability claim by a Data Subject or by a third party or any other claim in connection with the processing of data by the Processor as of this DPA, the Processor shall make every effort to support the Controller.

6. Subcontracting

(1) The Processor may outsource part of the processing activities pursuant to this DPA to Sub-processors that, as far as legally required, shall be subject to the contractual obligations resulting from art. 28 par. 4 GDPR.
The Processor currently commissions the following Sub-processors on the condition of a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR:

	A	B	C
1	Company subcontractor	Address/country	Service
2			
3			

(3) The transfer of personal data to any Sub-processor shall only take place after all above-mentioned conditions for the appointment of Sub-processors have been met.
(4) The Processor shall bear full responsibility and liability for the activities of its Sub-processors. Any change in the list of Sub-processors shall be notified to the Controller without undue delay, giving the Controller the option to object. In case of objection, the Processor retains the right to terminate the Contract with the Controller without notice.
(5) In particular, in case a Sub-processor should provide its services outside the

EU/EEA, the Processor shall ensure compliance with EU Data Protection Regulations by appropriate measures, as described at sec. 2 of this DPA.

7. Supervisory powers of the Controller

(1) Upon consultation with the Processor, the Controller has the right to carry out inspections or to have them carried out by an auditor to be designated on a case-by-case basis. The auditor shall have the right to assess the Processor's compliance with this DPA in his business operations by means of random checks, which are ordinarily to be announced in advance.
(2) The Processor shall allow the Controller to verify compliance with its obligations as provided by Article 28 GDPR**.** The Processor undertakes to give the Controller the necessary information on request and, in particular, to demonstrate the implementation of the technical and organizational measures.
(3) Evidence of such measures, which may not only concern the activities under this DPA, may also be provided by

- compliance with approved Codes of Conduct pursuant to Article 40 GDPR;
- certification according to an approved certification procedure in accordance with Article 42 GDPR;
- current auditor’s certificates, reports or excerpts from reports provided by independent bodies (e.g. auditor, data protection officer, IT security department, data protection auditor)
- a suitable certification by IT security or data protection auditing.

(4) The Processor may charge a reasonable fee to the Controller for enabling inspections.

8. Assistance to the Controller

(1) The Processor shall assist the Controller in complying with the obligations concerning the security of personal data, reporting of data breaches, data protection impact assessments and prior consultations set forth at Articles 32 to 36 of the GDPR, including

- ensuring adequate protection standards through technical and organizational measures, taking into account the type, circumstances and purposes of processing, the likelihood of data breaches and the severity of the risk to natural persons possibly resulting thereof
- ensuring immediate detection of infringements
- reporting data breaches without undue delay to the Controller
- assisting the Controller in answering to data subjects' requests or the exercise of their rights

(2) The Processor may claim a reasonable fee for support services which are not included in the description of the services and which are not attributable to failures on the part of the Processor.

9. Directive powers of the Controller

(1) The Processor shall not process any personal data under this DPA except on instructions from the Controller, unless required to do so by Union or Member State law.
(2) In case the Controller should require any change in the processing of personal data set forth by the documented instructions mentioned at sec. 2, the Processor shall immediately inform the Controller if it considers such changes likely to result in infringements to data protection provisions. The Processor may refrain from carrying out any activity that may result in any such infringement.

10. Liability

(1) Each party to this DPA commits to indemnify the other party for damages or expenses resulting from its own culpable infringement of this DPA, including any culpable infringement committed by its legal representative, subcontractors, employees or any other agents. Furthermore, each party commits to indemnify the other party against any claim exerted by third parties due to or in connection with any culpable infringement by the respectively other party.
(2) Art. 82 GDPR stays unaffected.

11. Deletion and return of personal data

(1) The Processor shall not create copies or duplicates of the data without the Controller's knowledge and consent, except for backup copies as far as they are necessary to ensure orderly data processing, as well as data required to meet regulatory data retention requirements.
(2) After conclusion of the provision of services, the Processor shall, at the Controller's choice, delete in a data-protection compliant manner or return to the Controller all the personal data collected and processed under this DPA, unless any applicable legal provision requires further storage of the personal data. In any case the Processor may retain all information necessary to demonstrate orderly and compliant processing activities beyond termination of the Contract, in accordance with the statutory retention periods.
(3) Documentation which is used to demonstrate orderly data processing in accordance with the DPA shall be stored beyond the contract term by the Processor in accordance with the respective retention periods. It may hand such documentation over to the Controller at the end of the contract duration to relieve the Processor of this contractual obligation.