Template  
Processing in accordance with Article 28 General Data Protection Regulation (GDPR) (as of: December 2020)

Agreement

between

................................................................................................  
the Data Controller – hereinafter referred to as the Controller

and

................................................................................................  
the Data Processor - hereinafter referred to as the Processor

**Please Note**

The following is a general model for a Controller-Processor agreement and must be adapted to the needs of the contracting parties in each individual case.

The specific provisions according to Article 28 Paragraph 3 GDPR should be incorporated into the Agreement in their entirety and be used as a Checklist. The alternatives applicable for the specific service relationship should be ticked. Empty fields are to be filled in as applicable to the specific requirements of each individual agreement. Systems of payment and liability conditions concerning the specific services of the Processor should be agreed in the main contract.

1. Subject-matter and duration of the Agreement

(1) Subject-matter of the Agreement

* The Subject-matter of the Agreement results from the Service Agreement/SLA/Order/Instruction …………….. dated …………., which is referred to here (hereinafter referred to as Service Agreement).

or

* The subject-matter of the Agreement regarding the processing of data is the execution of the following services or tasks by the Processor ……………………………………………………………………… (Definition of the services or tasks)

(2) Duration

* The duration of this Agreement corresponds to the duration of the Service Agreement.

or (specifically, if no Service Agreement regarding the Duration exists)

* The Processing will be authorised for one time execution only.

or

* The Duration of this Agreement is limited in time until ……….. .

or

* The Agreement is concluded for an unlimited period and can be terminated by either Party with a notice period of…… (time period) to ……. (deadline). This does not prejudice the right to termination of the contract without notice.

(3) This Agreement shall apply without prejudice to the preceding paragraph for as long as the Processor processes personal data of the Controller (including backups).

(4) Insofar as other arrangements on the protection of personal data arise from other agreements between the Controller and the Processor, this Agreement regarding the processing of personal data shall take precedence, unless the parties expressly agree otherwise.

1. Specification of the Agreement Details

(1) Nature and Purpose of the intended Processing of Data

* Nature and Purpose of Processing of personal data by the Processor for the Controller are precisely defined in the Service Agreement dated ………………. .

or

* Detailed description of the subject-matter with regard to the Nature and Purpose of the services provided by the Processor: ........................................

(2) Type of Data

* The type of personal data used is precisely defined in the Service Agreement under: …..

or

* The subject-matter of the processing of personal data comprises the following data types/categories (List/Description of the Data Categories)
  + Personal Master Data (Key Personal Data)
  + Contact Data
  + Key Contract Data (Contractual/Legal Relationships, Contractual or Product Interest)
  + Customer History
  + Contract Billing and Payments Data
  + Disclosed Information (from third parties, e.g. Credit Reference Agencies or from Public Directories...
  + Other: … (Please specify)

(3) Categories of Data Subjects

* The Categories of Data Subjects are precisely defined in the Service Agreement under: ..................................

or

* The Categories of Data Subjects comprise:
  + Customers
  + Potential Customers
  + Subscribers
  + Employees
  + Suppliers
  + Authorised Agents
  + Contact Persons
  + Other: …... (Please specify)

1. Technical and Organisational Measures

(1) The Processor shall take all necessary technical and organisational measures in its area of responsibility in accordance with Article 32 DS-GVO to protect personal data and shall provide the Controller the documentation for inspection [Annex 1]. If approved by the Controller, the documented measures become the basis of the Agreement.

(2) Insofar as the inspection/audit by the Controller reveals the need for amendments, such amendments shall be implemented by mutual agreement.

(3) The agreed Technical and Organisational Measures are subject to technical progress and further development. In this respect, it is permissible for the Processor to implement alternative adequate measures in the future. In so doing, the security level of the defined measures must not be reduced. The Controller shall be informed immediately of any significant changes which have to be documented by the Processor without delay.

*[OPTIONAL CLAUSE] The processing of personal data subject to this Agreement is not permitted in private homes (home and teleworking).*

1. Rights of the data subject

(1) The Processor shall support the Controller within its area of responsibility and as far as possible by means of appropriate technical and organisational measures in responding to requests from data subjects. The Processor must not on its own discretion respond to data subject requests concerning access to data, portability, rectification, erasure or the restriction of processing of data being processed on behalf of the Controller, but only on documented instructions from the Controller. Insofar as the Data Subject contacts the Processor directly, the Processor will immediately forward the Data Subject’s request to the Controller.

(2) Insofar as it is included in the scope of services, the right of access, to rectification, to restriction of processing, to erasure and to data portability shall be ensured directly by the Processor in accordance with documented instructions from the Controller.

1. Quality assurance and other duties of the Processor

(1) In addition to complying with the rules of this Agreement, the Processor shall comply with its own legal obligations under the GDPR; accordingly, the Processor ensures compliance with the following requirements in particular:

1. Confidentiality in accordance with Article 28 Paragraph 3 Sentence 2 Point b, Articles 29 and 32 Paragraph 4 GDPR. The Processor entrusts only such employees with the data processing outlined in this Agreement who have been bound to confidentiality and have previously been made aware of the data protection provisions relevant to their work. The Processor and any person acting under its authority who has authorised access to personal data, shall not process that data unless on instructions from the Controller, which includes the powers granted in this Agreement, unless required to do so by law.
2. The Controller and the Processor shall cooperate, on request, with the supervisory authority in performance of its tasks.
3. The Controller shall be informed immediately of any inspections and measures conducted by the supervisory authority, insofar as they relate to this Agreement. 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 Civil or Criminal Law, or Administrative Rule or Regulation regarding the processing of personal data in connection with this Agreement.
4. Insofar as the Controller is subject to an inspection by the supervisory authority, an administrative or summary offence or criminal procedure, a liability claim by a Data Subject or by a third party or any other claim or information request in connection with the processing by the Processor under this Agreement, the Processor shall make every effort to support the Controller.
5. The Processor shall periodically monitor the internal processes and the Technical and Organizational Measures to ensure that processing within its area of responsibility is in accordance with the requirements of applicable data protection law and the protection of the rights of the data subject.
6. Verifiability of the Technical and Organisational Measures conducted by the Controller as part of the Controller’s inspection powers referred to in item 8 of this Agreement.
7. The Processor shall report breaches of the protection of personal data to the Controller without delay in such a way that the Controller can fulfil its legal obligations, in particular in accordance with Articles 33 and 34 of the GDPR. It shall prepare documentation on the entire breach, which shall be made available to the Controller for further measures.
8. The Processor shall support the Controller in its area of responsibility and, as far as possible, to provide information to supervisory authorities and data subjects and shall make all relevant information available immediately to the Controller in this regard.
9. Insofar as the Controller is obliged to carry out a data protection impact assessment, the Processor shall support the Controller taking into account the type of processing and the information available to it. The same applies to any existing obligation to consult the competent data protection supervisory authority.

(2) This Agreement does not exempt the Processor from compliance with other requirements of the GDPR.

1. Subcontracting

(1) Subcontracting for the purpose of this Agreement is to be understood as meaning services which relate directly to the provision of the principal service. This does not include ancillary services commissioned by the Processor, such as telecommunication services, postal / transport services, cleaning or guarding services. IT services shall constitute a subcontracting relationship if they are provided for IT systems which are used for this Agreement. The Processor shall, however, be obliged to make appropriate and legally binding contractual arrangements including technical and organisational measures and take appropriate inspection measures to ensure the data protection and the data security of the Controller's data, even in the case of outsourced ancillary services.

(2) The Processor may commission subcontractors (additional processors) only after prior explicit written or documented authorisation from the Controller.

a) □ Subcontracting is not permitted.

b) □ The Controller agrees to the commissioning of the following subcontractors stipulated in Annex 2 on the condition of a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR with the subcontractor:

The contractual agreement shall be presented to the Controller at the Controller's request, with the exception of business clauses not related to data protection law.

c) □ Outsourcing to subcontractors or

□ Changing the existing subcontractor

are permissible when:

* the Processor submits such an outsourcing to a subcontractor to the Controller in writing or in text form with appropriate advance notice, but not less than 14 days; and
* the Controller has not objected to the planned outsourcing in writing or in text form by the date of handing over the data to the Processor; and
* the subcontracting is based on a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR.

(3) The transfer of personal data from the Controller to the subcontractor and the subcontractor’s commencement of the data processing shall only be undertaken after compliance with all requirements has been achieved. Compliance with and implementation of the technical and organisational measures at the subcontractor shall be inspected by the Processor in advance of the processing of personal data, taking into account the risk at the subcontractor, and then on a regular basis. The Processor shall make the inspections results available to the Controller upon request. The Processor shall also ensure that the Controller can exercise its rights under this contract (in particular its inspection rights) directly against the subcontractors.

(4) If the subcontractor provides the agreed service outside the EU/EEA, the Processor shall ensure compliance with EU Data Protection Regulations by appropriate measures. The same applies if service providers are to be used within the meaning of Paragraph 1 Sentence 2.

(5) Further outsourcing by the subcontractor

* Is not permitted;
* Requires the express consent of the main Controller (at the minimum in text form);
* Requires the express consent of the Processor (at the minimum in text form);

All contractual provisions in the contract chain shall be communicated to and agreed with each and every additional subcontractor.

1. International data transfers

(1) Any transfer of personal data to a third country or to an international organisation requires documented instructions from the Controller and compliance with the requirements for the transfer of personal data to third countries pursuant to Chapter V of the GDPR.

* The undertaking of the contractually agreed Processing of Data shall be carried out exclusively within a Member State of the European Union (EU) or within a Member State of the European Economic Area (EEA).
* The Controller allows data to be transferred to a third country. Annex 2 specifies the measures to ensure an adequate level of data protection under Article 44 et seq. GDPR within the framework of the subcontracting.

(2) Insofar as the Controller instructs a data transfer to third parties in a third country, the Controller shall be responsible for compliance with Chapter V of the GDPR.

1. Supervisory powers of the Controller

(1) The Controller has the right, after consultation with the Processor, to carry out inspections or to have them carried out by an auditor to be designated in each individual case. It has the right to convince itself of the compliance with this Agreement by the Processor in its business operations during normal business hours by means of random checks, which are ordinarily to be announced in good time.

(2) The Processor shall ensure that the Controller is able to verify compliance with the obligations of the Processor in accordance with Article 28 GDPR**.** The Processor undertakes to give the Controller the necessary information on request and, in particular, to demonstrate the execution of the Technical and Organizational Measures.

(3) Evidence of the Technical and Organisational measures for compliance with data protection requirements in general as well as those relating to this specific Agreement, may 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 privacy auditor, quality auditor)
* A suitable certification by IT security or data protection auditing (e.g. according to BSI-Grundschutz (IT Baseline Protection certification developed by the [German](https://en.wikipedia.org/wiki/Germany) Federal Office for Security in Information Technology (BSI)) or [ISO/IEC 27001](https://de.wikipedia.org/wiki/ISO/IEC_27001)).

1. Authority of the Controller to issue instructions

(1) The Processor shall process personal data only on the basis of documented instructions from the Controller, unless it is obliged to process such data under the law of the Member State or under Union law. The Controller shall immediately confirm oral instructions (at the minimum in text form). The Controller's initial instructions shall be determined by this Agreement.

(2) The Processor shall inform the Controller immediately if he considers that an instruction violates Data Protection Regulations. The Processor shall then be entitled to suspend the execution of the relevant instructions until the Controller confirms or changes them.

1. Deletion and return of personal data

(1) Copies or duplicates of the data shall never be created without the knowledge of the Controller, with the exception of back-up copies as far as they are necessary to ensure orderly data processing, as well as data required to meet regulatory requirements to retain data.

(2) After conclusion of the contracted 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 or – subject to prior consent – destroy all documents, processing and utilization results, and data sets related to the Agreement that have come into its possession, in a data-protection compliant manner. The same applies to any and all connected test, waste, redundant and discarded material. The log of the destruction or deletion shall be provided on request.

Appendix 1 - Technical and Organisational Measures

Description of the Technical and Organisational measures taken by the Processor, taking into account the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

Where necessary,

[Description of measures for pseudonymisation and encryption of personal data]

[Description of measures to ensure the continuous confidentiality, integrity, availability and resilience of systems and services related to the processing]

[Description of measures to ensure the availability of personal data and access to personal data in a timely manner in the event of a physical or technical incident]

[Description of measures to ensure a procedure for periodic review, assessment and evaluation of the effectiveness of the Technical and Organisational measures taken to ensure the security of processing]

[Description of measures for user identification and authorisation]

[Description of measures for the protection of personal data during transmission]

[Description of measures for the protection of personal data during their storage]

[Description of measures to ensure physical security of locations where personal data are processed]

[Description of measures for the protection of personal data during home or teleworking][[1]](#footnote-1)

[Description of event logging requirements (e.g. for user authorisation or data input, modification or deletion)]

[Description of technical-organisational measures within the framework of the Processor's support obligations (e.g. concerning data subject rights)]

Appendix 2 - Authorised subcontractors

|  |  |  |  |
| --- | --- | --- | --- |
| **Subcontracting company** | **Address/Country** | **Service** | **Appropriate safeguards in case of a transfer of personal data to a third country** |
|  |  |  |  |
|  |  |  |  |

1. Not to be described if home working and teleworking have been prohibited in accordance with the optional clause in section 3 of the model contract. [↑](#footnote-ref-1)