# DATA PROCESSING AGREEMENT IN ACCORDANCE WITH ART. 28 GENERAL DATA PROTECTION REGULATION (GDPR)

hereinafter referred to as agreement

between

_____

- the controller - hereinafter referred to as data controller -

and

_____

- the processor, hereinafter referred to as the data processor –

When applicable: authorised representative in accordance with Article 27 GDPR:

_____

hereinafter individually or jointly referred to as: "Parties"

**Preamble**

On_____, the parties concluded a contract for the provision of services in accordance with personal data (hereinafter: "main contract"). This contract specifies the obligations of the parties to data protection arising from the main contract. It applies to all activities relating to the main contract in which the data processor, employees of the data processor or agents of the data processor may come into contact with personal data of the principal.

## 1 Subject matter, duration, type, scope and purpose of processing (Art. 28 paragraph 3 Point. 1 GDPR)

(1) The data processor processes personal data on behalf of the data controller in order to fulfil his contractual obligations towards the data controller. The subject, purpose, duration, nature and scope of the processing, including the categories of data subjects, are set out in Appendix 1.

## 2 Obligations and rights of the data controller (Art. 28 paragraph 3 sub-paragraph 1 GDPR)

(1) The obligations and rights of the data controller according to Art. 28 paragraph 3 sub-paragraph 1 GDPR result from the main contract and this contract.

## 3 Obligation of persons engaged (Art. 28 paragraph 3 sub-paragraph 2 point b GDPR)

(1) The data processor shall oblige persons employed or authorised to process the personal data in advance to maintain confidentiality and data secrecy or shall ensure that they are subject to an appropriate statutory duty of confidentiality with regards to the personal data. The data processor and any person subject to the data processor 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.

## 4 Technical and organizational measures (Art. 28 paragraph 3 sub-paragraph 2 point c GDPR)

(1) The data processor 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 regards to the concrete execution of the contract, and shall hand them over to the data controller for inspection. If accepted by the data controller, the documented measures become the basis of the order. If the audit/audit of the data controller reveals a need for adjustment, this must be implemented by mutual agreement.
(2) The data processor must provide security in accordance with Art. 28 paragraph 3 point c and Art. 32 GDPR, particularly in connection with Art. 5 paragraphs 1 and 2 GDPR. Overall, the measures to be taken are measures of data security and to ensure a level of protection appropriate to the risk with regards to the confidentiality, integrity, availability and resilience of the systems. The state of the art, the implementation costs and the type, scope and purpose 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 paragraph 1 GDPR must be taken into account [details in Appendix 2].
(3) The technical and organisational measures are subject to technical progress and further development. In this respect, the data processor is permitted to implement alternative adequate measures. The safety level of the defined measures must not be undershot. Significant changes must be documented.

## 5 Sub-Processing

(1) Sub-processing relationships within the meaning of this provision shall be understood to mean those services which relate directly to the provision of the main service. This does not include ancillary services which the data processor 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 data controller's data, the data processor is obliged to take appropriate and legally compliant contractual agreements and control measures, even in the case of outsourced ancillary services. The data processor shall first impose on the sub-processor by contract or by any other applicable legal instrument under the law of the European Union or of the Member State concerned the same data protection obligations as those laid down between him and the contracting entity in this contract or by any other applicable legal instrument of European Union law.
(2) The data controller agrees to the assignment of the subcontractors listed in Appendix 3 subject to the condition of a contractual agreement in accordance with Art. 28 paragraphs (2-4) of the GDPR. The use of further subcontractors not listed in Appendix 3 shall require the prior written consent of the data controller in order to be lawful. The data controller may not refuse such approval improperly or without reason.
(4) The transfer of the data controller's personal data to the sub-processor and his first action are only permitted if all requirements for subcontracting are met.
(5) If the sub-processor performs the agreed service outside the EU/EEA, the data processor shall ensure the admissibility under data protection law through appropriate measures.

## 6 Place of processing

(1) 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, or Switzerland. 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. GDPR are fulfilled. The data controller hereby expressly consents that the contractually agreed data processing can be transferred to Switzerland and can take place there.

## 7 Support of the data controller in the fulfilment of data protection obligations

(1) The data processor shall, as far as possible, assist the contracting authority in responding to requests from data subjects, informing data subjects about the processing of their personal data and implementing the rights of data subjects with regards to the data processed. The data processor does not respond to requests for information and other requests (e.g. requests for deletion, correction or restriction of personal data) from affected persons himself, but instead refers the affected persons to the data controller in this respect.
(2) The data processor shall assist the contracting authority, taking into account the type of processing and the information available to him, in implementing and implementing technical and organisational measures taken by the contracting authority, in reporting data protection violations to the data protection supervisory authorities as required by law, in notifying the persons concerned of data protection violations as required by law, in the case of legally required obligations for data protection impact assessments and legally required consultations with the data protection supervisory authority.
(3) For support services that are not included in the main contract or are not attributable to misconduct on the part of the data processor, the data processor may claim compensation.

## 8 Data rectification, restriction and deletion

(1) The data processor may not rectify, delete or restrict the processing of the data processed in the order on his own authority, but only after the documented instructions of the data controller. Where a data subject contacts the data processor directly in this respect, the data processor shall immediately forward this request to the contracting authority.
(2) Insofar as the scope of services includes, the deletion concept, the right to oblivion, correction, data portability and information must be ensured directly by the data processor in accordance with the documented instructions of the data controller.

## 9 Deletion and return of personal data

(1) Copies or duplicates of the data will not be made without the knowledge of the data controller. Excluded from this are backup copies, insofar as they are necessary to guarantee proper data processing, as well as data which are necessary with regards to compliance with legal storage obligations.
(2) After completion of the contractually agreed work or earlier upon request by the data controller - at the latest upon termination of the main contract - the data processor must hand over to the data controller 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 report must be submitted without request.
(3) Documentation that serves as proof of orderly and proper data processing must be kept by the data processor after the end of the contract in accordance with the respective retention periods. He can hand them over to the data controller at the end of the contract in order to relieve the data controller.

## 10 Data protection obligations of the data processor, proof of compliance and control rights (Art. 28 paragraph 3 sub-paragraph 2 point h and Art. 31 GDPR)

(1) The data controller has the right to carry out inspections in consultation with the data processor or to have them carried out by inspectors to be appointed in individual cases. He has the right to satisfy himself of the data processor'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 data processor ensures that the data controller can convince himself of the compliance with the obligations of the data processor according to Art. 28 GDPR. The data processor undertakes to provide the data controller with the necessary information on request and in particular to provide evidence of the implementation of the technical and organisational measures.
(3) Proof of such measures, which do not only concern the specific order, can be provided by

- compliance with approved rules of conduct in accordance with Art. 40 GDPR;
- certification according to an approved certification procedure according to Art. 42 GDPR;
- current certificates, reports or report extracts from independent bodies (e.g. auditors, auditors, data protection officers, IT security department, data protection auditors, quality auditors);
- suitable certification through IT security or data protection audits (e.g. according to BSI-Grundschutz).

(4) The data processor shall regularly monitor the internal processes and the technical and organisational measures taken to ensure that processing within his area of responsibility is carried out in accordance with the requirements of the applicable data protection law and that the rights of the data subject are protected.

(5) In addition to complying with the provisions of this contract, the data processor shall have legal obligations pursuant to Articles 28 to 33 GDPR; in this respect, the data processor shall in particular ensure compliance with the following requirements:

The data processor shall appoint a data protection officer to the extent required by law
**Data Protection Officer of data processor:**
**Mr**
**Kargl Rolf-Dieter**
**dsb@trivadis.com**

(6) Maintaining confidentiality in accordance with Art. 28 paragraph 3 sub-paragraph 2 point b, 29, and 32 paragraph 4 GDPR. In carrying out the work, the data processor shall only employ employees who are bound to confidentiality and who have been familiarised beforehand with the data protection provisions relevant to them. The data processor and any person subject to the data processor who has access to personal data may process such data only in accordance with the instructions of the contracting authority, including the powers granted in this contract, unless required to do so by law.
(7) Implementation and compliance with all technical and organisational measures required for this order in accordance with Art. 28 paragraph 3 sub-paragraph 2 point c and 32 GDPR [details in Appendix 2].
(8) The data processor keeps a list of processing activities in accordance with Art. 30 paragraph 2 GDPR and makes this available to the contracting authority on request.
(9) The data processor shall provide the principal with all information necessary to prove compliance with his contractual and statutory obligations as a contract processor. It permits and enables the data controller and his authorised inspectors to carry out appropriate inspections - including inspections - and contributes to this to an appropriate extent. Checks must be reported to the data processor at least 30 calendar days in advance.
(10) The data processor may assert a claim for remuneration in order to enable the data controller to carry out inspections. (11) The data processor shall immediately inform the contracting authority of any control actions and measures taken by the supervisory authority in so far as they relate to this contract. This also applies if a competent authority investigates within the framework of administrative or criminal proceedings with regards to the processing of personal data during order processing at the data processor.
(12) Where the contracting authority, for its part, is subject to inspection by the supervisory authority, administrative or criminal proceedings, the liability of a person concerned or of a third party or any other claim in connection with the processing of the contract with the data processor, the data processor must support it to the best of its ability.

## 11 Processing of personal data only on documented instructions (Art. 28 paragraph 3 sub-paragraph 2 point a GDPR)

(1) The data processor processes and transmits personal data of the data controller only on documented instructions of the data controller. This applies in particular to the transfer of the data controller's personal data to a recipient in a third country or to an international organisation; this may only take place with the express permission of the data controller and only if the requirements of Chapter V of the GDPR are fulfilled. The data controller hereby expressly consents to the transfer of personal data to and processing in Switzerland.
(2) The instructions are initially laid down in this contract and the main contract and can then be amended, supplemented or replaced by the data controller in writing or in text form by individual instructions.

(3) The data processor may also process and communicate the contracting entity's personal data if he is required to do so by the law of the European Union or of a Member State. In that case, it shall inform the contracting entity of those legal requirements, unless the law in question prohibits such notification on grounds of an important public interest.

## 12 Information on instructions contrary to data protection, the data controller's authority to issue instruction (Art. 28 paragraph 3 sub-paragraph 2 point a GDPR and Art. 28 paragraph 3 sub-paragraph point 3 GDPR)

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

## 13 Notification in the event of breaches by the data processor

(1) The data processor shall immediately inform the principal if third parties gain unlawful knowledge of the personal data or in the event of other serious violations by the data processor or persons employed by the data processor within the scope of the order of provisions for the protection of the principal's personal data or stipulations made in this contract. He shall take the necessary measures to secure the data and to mitigate possible adverse consequences of the persons concerned and shall consult with the data controller without delay. The above notification obligation always applies if the possibility cannot be ruled out that the violation will result in a reporting obligation on the part of the data controller pursuant to Art. 33 paragraph 1 GDPR or Art. 34 paragraph 1 GDPR.

## 14 Other obligations and final provision

(1) The data controller shall name the contact person for any data protection issues arising within the framework of the contract. The data protection officer of the data controller is:

Name: _____

E-Mail: _____

(2) Should the data of the data controller be endangered at the data processor by seizure or confiscation, by insolvency or composition proceedings, by requests for disclosure in connection with legal proceedings or by other events or measures of third parties, the data processor must inform the data controller immediately. The data processor shall immediately inform all persons responsible in this context that the sovereignty and ownership of the data lies exclusively with the data controller as the person responsible within the meaning of data protection law.

(3) Changes and supplements to this agreement and all its components - including any assurances of the data processor - require a written agreement, which can also be made in electronic form, and the express indication that this agreement is an amendment or addition. This also applies to the waiver of this formal requirement.
(4) In the event of any contradictions, the provisions of this agreement on data protection take precedence over the provisions of the main contract.
(5) In the event of any contradictions in this Data Processing Agreement to the German Data Processing Agreement, the current German version of the Data Processing Agreement shall apply.

| | Data Processor | Data Processor | Data Processor |
|---|---|---|---|
| Name | | | Rolf-Dieter Kargl |
| Function | | | DPO |
| Place / Date | | | Vienna, |
| | **Signature** | **Signature** | **Signature** |
| | **Controller** | **Controller** | **Controller** |
| Name | | | |
| Function | | | |
| Place / Date | | | |
| | **Signature** | **Signature** | **Signature** |

## APPENDIX 1 – DATA PROCESSING DETAILS

### Subject matter and purpose of processing

*(Note: subject of the order, concrete description of the services)*

_____

### Type of personal data

The following personal data will be processed:

- ☐ Personal Master Data (Key Personal Data)
- ☐ Contact Data (e.g. phone number, e-mail)
- ☐ Application data (e.g. curriculum vitae, certificate, possibly degree of disability)
- ☐ 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:

### Categories of data subjects

The categories of data subjects include:

- ☐ Customers
- ☐ Candidates
- ☐ Interested parties
- ☐ Suppier
- ☐ Subscribers
- ☐ Employees
- ☐ Data processors
- ☐ Authorised Agents
- ☐ Contact Persons (e.g. intermediary)
- ☐ Other - Please specify:

**Duration of processing**

☐ The duration of this agreement (term) corresponds to the term of the main contract.

☐ Duration of processing is:

**Sub-Processors**

| Sub-Processor (Company Name) | Contact Details | Place of Processing | Description of Service |
|---|---|---|---|
| | | | |
| | | | |

**Technical contact person**

Technical contact person of data controller:

Name:

Function:

Telephone:

E-Mail:

Technical contact person of data processor:

Name:

Function:

Telephone:

E-Mail:

trivadis
Part of Accenture

## APPENDIX 2 – TECHNICAL AND ORGANIZATIONAL MEASURES

### Confidentiality (Art. 32 paragraph 1 point b GDPR)

| | |
|---|---|
| **Physical access control**<br>No unauthorised access to Data Processing Facilities, e.g.: magnetic or chip cards, keys, electronic door openers, facility security services and/or entrance security staff, alarm systems, video/CCTV Systems; | ▪ Card-based personalized access control systems with access authorization for authorized employees only,<br>▪ Instructions for handling access controls,<br>▪ Guidelines for accompanying and marking guests in the building<br>▪ Server in lockable server cabinets, IT department manage keys,<br>▪ Organizational statement for issuing keys,<br>▪ Closure of laptops in cabinets after office hours,<br>▪ Locking of the building after closing time as well as security by alarm system. |
| **Electronic Access Control**<br>No unauthorised use of the Data Processing and Data Storage Systems, e.g.: (secure) passwords, automatic blocking/locking mechanisms, two-factor authentication, encryption of data carriers/storage media; | ▪ Server systems can only be administered with console password or via password-protected, encrypted connection<br>▪ Data encryption<br>▪ Data controller systems can only be used after password-based network authentication<br>▪ Temporary Blocking of the user account after five failed login attempts<br>▪ Automatic, password-protected screen and computer lock after 10 minutes<br>▪ Unique assignment of user accounts to users, no impersonal collective accounts ("AZUBI1")<br>▪ Guideline for secure, proper handling of passwords/smart cards<br>▪ Automated standard routines for regular updates of protection software (e.g. virus scanners) |
| **Internal Access Control**<br>(permissions for user rights of access to and amendment of data) No unauthorised Reading, Copying, Changes or Deletions of Data within the system, e.g. rights authorisation concept, need-based rights of access, logging of system access events; | ▪ Data encryption<br>▪ Separation of authorisation (organisational) by department head / management / management and allocation of authorisation (technical) by IT department<br>▪ Network drives with access only for authorized users (groups) |

| | |
|---|---|
| **Isolation Control**<br>The isolated Processing of Data, which is collected for differing purposes, e.g. multiple Data controller support, sandboxing; | ▪ The data of the DATA CONTROLLER and other data controllers are processed as far as possible by different employees of the service provider.<br>▪ An authorization concept exists that takes account of the separate processing of the DATA CONTROLLER data from data from other data controllers.<br>▪ The authorization mechanisms available in the systems used enable the exact implementation of the specifications of the authorization concept |

## Integrity (Art. 32 paragraph 1 point b GDPR)

| | |
|---|---|
| **Data Transfer Control**<br>No unauthorised Reading, Copying, Changes or Deletions of Data with electronic transfer or transport, e.g.: Encryption, Virtual Private Networks (VPN), electronic signature; | ▪ Sending personal data, e.g. by encrypted e-mail<br>▪ Data encryption<br>▪ Line encryption |
| **Data Entry Control**<br>Verification, whether and by whom personal data is entered into a Data Processing System, is changed or deleted, e.g.: Logging, Document Management; | ▪ Contractual restriction of the work with the DATA CONTROLLERS personal data to the service provider's employees working in connection with services under the contract. |

## Availability and Resilience (Art. 32 paragraph 1 point b GDPR)

| | |
|---|---|
| **Availability Control**<br>Prevention of accidental or wilful destruction or loss, e.g.: Backup Strategy (online/offline; on-site/off-site), Uninterruptible Power Supply (UPS), virus protection, firewall, reporting procedures and contingency planning; | ▪ Complete backup and recovery concept with daily backup and disaster-proof storage of data carriers<br>▪ Expert use of protection programs (virus scanners, firewalls, encryption programs, SPAM filters) and written conception of their use (virus protection concept, etc.)<br>▪ Use of uninterruptible power supply |
| **Order or Contract control**<br>No processing of data within the meaning of Art. 28 GDPR without corresponding instructions from the data controller, e.g.: Clear contract design, formalized order management, strict selection of service provider, obligation to convince in advance, follow-up checks. | ▪ The contract contains detailed information on the type and scope of the commissioned processing and use of personal data of the DATA CONTROLLER<br>▪ The contract contains detailed information on the purpose of the personal data of the DATA CONTROLLER as well as a prohibition of use by the service provider outside of the order formulated in writing.<br>▪ The service provider has appointed a company data protection officer and, through the data protection organisation, ensures his appropriate and effective integration into the relevant company processes. |

| | |
|---|---|
| **Rapid Recovery**<br>(Art. 32 paragraph 1 point c GDPR); e.g. through: Backup concept, redundant data storage, double IT infrastructure, shadow data center | ▪ Complete backup and recovery concept with daily backup and disaster-proof storage of data carriers |

## APPENDIX 3 – STANDARD CONTRACTUAL CLAUSES AND ADDITIONAL MEASURES REGARDING DATA TRANSFER TO THIRD COUNTRIES

*(Note: Only applicable for data transfers to third countries without an EU adequacy decision. Has to be filled out and signed)*

### EU standard contractual clauses (in the version valid at the time of conclusion of the contract)

CELEX_32021D0914_EN_TXT.pdf

### Additional measures regarding data transfer to third countries

(1) If Processor receives a legally effective request from law enforcement authorities ("Law Enforcement") or any other third party seeking the disclosure of Personal Data that belongs to Controller, Processor is obligated to promptly notify Controller of such request and direct Law Enforcement or third party to seek information directly from Controller and not Processor.

(2) If Processor is legally prohibited from notifying Controller and redirecting Law Enforcement or third party, Processor is obligated to challenge the legal prohibition to enable redirection or notice to Controller. If such challenge is unsuccessful, it is the common understanding of the Parties that Processor shall initiate litigation proceedings.

(3) Processor will not provide any third party: (a) direct, indirect, blanket, or unfettered access to Personal Data; (b) platform encryption keys used to secure Processed Data or the ability to break such encryption; or (c) access to Personal Data if Processor is aware that the data is to be used for purposes other than those stated in the third party's request. In support of the above, Processor may provide Controller's basic contact information to the third party.

(4) The Parties agreed that they will enter into additional agreements regarding additional protections measures with regard to transfer of personal data to third countries as required by local or European data protection authorities.