Data Protection Agreement for Job Data Processing pursuant to Article 28 of the EU General Data Protection Regulation (GDPR)

At the behest of	processed by
	Data Virtuality GmbH Katharinenstr. 15 04109 Leipzig
(hereinafter, the "**Client**")	(hereinafter, the "**Contractor**")

(hereinafter referred to together as the **"Parties**").

§ 1 General remarks

1. The Contractor shall process personal data on behalf of the Client in the terms of Articles 4(8) and 28 of Regulation (EU) 2016/679 - General Data Protection Regulation (GDPR). This Agreement stipulates the rights and duties of the Parties in connection with the processing of personal data.
2. In the event of any contradictions, the provisions of this Agreement with all its components take precedence over the provisions of the associated main contract.
3. Insofar as the term "data processing" or "processing" (of data) is used in this Agreement, the definition of "processing" in the terms of Article 4(2) GDPR shall apply.
4. The Contractor hereby agrees to carry out the job data processing only in member states of the European Union (EU) or the European Economic Area (EEA).

§ 2 Subject of contract

1. The object, nature and purpose of the processing, the nature of the personal data and the categories of data subjects are set out in **Annex 1** to this Agreement.
2. The duration of the job processing shall correspond to the term of the main contract. Reference is made to thereto.

§ 3 Rights and duties of the Client

1. The Client shall be the data controller in the terms of Article 4(7) GDPR for the job data processing by the Contractor.
2. As the data controller, the Client shall be responsible for ensuring that the rights of the data subjects are safeguarded.
3. The Client shall have the right to issue supplementary instructions to the Contractor regarding the type and scope of and procedure for data processing. Verbal instructions must be confirmed immediately in text form. The Client shall name persons authorised to issue instructions in **Annex 1**. In the event the persons authorised to issue instructions change at the Client, the Client shall inform the Contractor of this in text form.

§ 4 General duties of the Contractor

1. The Contractor shall process personal data exclusively within the framework of the arrangements made and/or in compliance with any supplementary instructions issued by the Client. Excluded from this shall be provisions of law which may oblige the Contractor to process the data in another way. In such case, the Contractor shall inform the Client of such legal requirements prior to processing, unless the law concerned prohibits such notification on grounds of an important public interest. The purpose, type and scope of data processing shall otherwise be exclusively

determined by this Agreement and/or the instructions of the Client. Any data processing deviating from this shall be prohibited to the Contractor.

2. The Contractor shall inform the Client without delay if an instruction issued by the Client violates provisions of law in its opinion. The Contractor shall be entitled to suspend the execution of the relevant instruction until it has been confirmed or changed by the Client. The Contractor may at all times refuse to carry out instructions that are obviously contrary to data protection law.
3. The Contractor shall name to the Client in **Annex 1** person(s) who is/are authorised to receive instructions from the Client. In the event the persons authorised to receive instructions change at the Contractor, the Contractor shall inform the Client of this in text form.

§ 5 Notification duties of the Contractor

1. The Contractor is obliged to notify the Client without delay of any violation of data protection regulations or of the contractual agreements made and/or the Client's instructions issued which transpires in the course of the data processing by the Contractor or by other persons involved in the processing. This shall also apply to any violation of the protection of the personal data processed by the Contractor on behalf of the Client.
2. Furthermore, the Contractor shall inform the Client without delay if a supervisory authority in accordance with Article 58 GDPR takes action against the Contractor and this may also concern scrutiny of the processing which the Contractor performs on behalf of the Client.
3. The Contractor shall inform the Client without delay if data subjects assert their rights as data subjects against the Contractor.
4. The Contractor is aware that the Client may be subject to a notification duty in accordance with Articles 33 and 34 GDPR. The Contractor shall support the Client in the implementation of the notification duties. In particular, the Contractor shall notify the Client of any unauthorised access to personal data processed on behalf of the Client, disruptions in the operating process or other irregularities in the handling of the Client’s personal data without delay as soon as the access becomes known. The Contractor's notification to the Client must contain the following information in particular:
    - a description of the nature of the personal data protection breach, indicating, as feasible, the categories and approximate number of data subjects, the categories and approximate number of personal data sets concerned;
    - a description of the likely consequences of the breach of personal data protection;
    - 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.

§ 6 Client’s duties to cooperate

1. The Contractor shall support the Client in its duty to respond to requests for the rights of data subjects to be safeguarded in accordance with Articles 12 to 23 GDPR. In particular, the Contractor shall ensure that the information required in this respect is provided to the Client without delay, so that the Client can fulfil its obligations under Article 12(3) GDPR in particular. Insofar as the cooperation of the Contractor is necessary for the protection of the rights of the data subjects (particularly to information, rectification, blockage or erasure) by the Client, the Contractor shall take the necessary measures in accordance with the Client's instructions. As feasible, the Contractor shall support the Client with suitable technical and organisational measures to enable the Client to comply with its obligation to respond to requests to safeguard the rights of the data subjects.
2. The Contractor shall assist the Client in complying with the duties set out in Articles 35 to 36 GDPR, with due regard to the nature of the processing and the information available to the Contractor.

§ 7 Controlling rights of the Client

1. The Client shall have the right to examine the Contractor's compliance with the provisions of law on data protection and/or the compliance with the contractual provisions agreed between the Parties and/or the compliance by the Contractor with the Client's instructions to the extent necessary or to have such compliance examined by commissioned auditors.
2. The Contractor shall be obliged to provide information to the Client, insofar as this is necessary for the performance of the examination in the terms of Paragraph 1.
3. The Client and/or the commissioned auditor may, after prior notification with a reasonable period of notice, carry out the examination in the terms of Paragraph 1 during normal business hours. In doing so, the Client shall ensure that the checks are only carried out to the extent necessary to avoid disproportionately disrupting the Contractor's operations through the checks. The Parties assume that an examination will be necessary at most once a year. Further checks must be justified by the Client by stating reasons.
4. Proof of compliance with the technical and organisational measures may be supported by the submission of a suitable, up-to-date confirmation, reports or report extracts from independent bodies (e.g. independent auditors, internal auditors, data protection officers, IT security department, data protection auditors or quality auditors) or suitable certification, provided the audit report enables the Client to satisfy itself in an appropriate fashion that the technical and organisational measures pursuant to **Annex 2** to this Agreement have been complied with. This shall not affect the right of the Client to carry out an on-site check. The Client is aware that an on-site check in computer centres can only be carried out in justified exceptional cases.

§ 8 Subcontracting relations

1. The Contractor shall be entitled to use the subcontractors listed in **Annex 1** to this Agreement as further processors in the terms of Article 28(4) GDPR for job processing of data.
2. The following terms and conditions shall apply to the change of subcontractors or the commissioning of further subcontractors:
   - The Contractor shall ensure that the provisions agreed in this Agreement and any supplementary instructions of the Client shall also apply to the subcontractor.
   - The Contractor must conclude a job processing agreement with the subcontractor which complies with the provisions of Article 28 GDPR. In addition, the Contractor must impose the same personal data protection duties on the subcontractor as those established between the Client and the Contractor. In particular, the technical and organisational measures to be agreed with the subcontractor must provide at least the same level of protection.
   - The Contractor shall inform the Client without delay of any intended change with regard to the involvement of new subcontractors or the replacement of existing subcontractors (“Notice of Change"), thereby giving the Client the opportunity to object to such changes (Article 28(2), Sentence 2 GDPR). The Notice of Change must be sent to the persons of the Client who are authorised to issue instructions.
   - If no objection is made by the Client within two weeks after receipt of the Notice of Change, the change shall be considered approved.
   - An objection can be retracted by the Client at any time in text form.
   - If the Client has raised an objection to a subcontractor and if a mutually agreed solution cannot be found between the Client and the Contractor, the Client and the Contractor shall have a special right of termination. The Contractor shall take the interests of the Client into account in the termination period.
5. The following are not to be regarded as subcontracting relationships in the terms of Paragraphs 1 to 5: services which the Contractor uses as a strictly ancillary service from third parties in order to carry out the business activity. These include, for example, cleaning services, strictly telecommunications services without any specific relation to services which the Contractor provides for the Client, postal and courier services, transport services, security services. The Contractor shall nevertheless be obliged, even in the case of ancillary services provided by third parties, to ensure that appropriate precautions and technical and organisational measures have been taken to warrant the protection of personal data. The maintenance and servicing of IT systems or applications shall constitute a subcontracting relationship and job processing in the terms of Article 28 GDPR if the maintenance and testing concerns IT systems that are also used in connection with

the provision of services for the Client and if personal data processed on behalf of the Client can be accessed during the maintenance.

§ 9 Confidentiality obligation

1. When processing data for the Client, the Contractor shall be obliged to maintain confidentiality about data that it receives or becomes aware of in connection with the order.
2. The Contractor has familiarised his employees with the provisions of data protection applicable to them and has obliged them to maintain confidentiality.

§ 10 Technical and organisational measures

1. The Contractor undertakes towards the Client to comply with the technical and organisational measures required to comply with the applicable data protection regulations. This shall include in particular the requirements of Article 32 GDPR.
2. The status of the technical and organisational measures existing at the time of conclusion of this Agreement is attached to this Agreement as **Annex 2**. The Parties agree that changes to the technical and organisational measures may be necessary to adapt to technical and legal conditions. Significant changes must be documented and made available to the Client on request. The Client shall be entitled at any time to review the arrangement reached with regard to the technical and organisational measures or to have such arrangement reviewed by an expert third party.

§ 11 Cessation

After cessation of this Agreement, the Contractor shall, at the discretion of the Client, return to the Client or delete in accordance with data protection regulations all documents, data and created processing or usage results that have come into its possession in connection with the contractual relationship. The deletion must be documented in an appropriate fashion. Any statutory storage duties or other duties to save data shall not be prejudiced hereby.

§ 12 Liability and damage compensation

1. The Client and the Contractor shall be liable to the data subjects in accordance with the provisions of Article 82 GDPR.
2. If a data subject asserts a damage compensation claim against one Party due to a violation of data protection regulations, the Party against whom recourse has been taken must inform the other Party of this immediately.
3. The Parties shall assist each other in defending against damage compensation claims of data subjects, unless this would jeopardise the legal position of one Party in relation to the other Party or the supervisory authority.

§ 13 Final provisions

1. Should any provision of this Agreement be or become invalid, this shall not affect the validity of the remainder of this Agreement. Another provision that most closely approximates the spirit and financial significance of the invalid provision shall then be considered as agreed between the Parties.

2. Any modifications of or additions to this Agreement, the respective individual contract and all the components thereof must be made in writing. This shall also apply to any waiver of this requirement for the written form.

3. The defense of a retention right in the terms of § 273 of the Civil Code shall be excluded with regard to the processed data and the associated data carriers.

4. The legal relations of the Parties shall be subject to the law of the Federal Republic of Germany to the exclusion of the UN Convention on Contracts for the International Sale of Goods and to the

exclusion of those rules of German law that refer to a legal system other than the German legal system.

5. For all disputes arising from or in connection with this Agreement, the jurisdiction agreement in the main contract shall apply, as permitted by law.

6. If the regulatory content of individual provisions of this Agreement extends beyond the term of contract, such provisions shall remain in effect after the end of the term of contract.

7. The annexes attached to this Agreement shall form an integral component hereof.

Annex 1: Specification of the job content

Annex 2: Technical and organisational measures

Place and date	Place and date
Client	Contractor
Name/ signature/ company stamp	Name/ signature/ company stamp

Annex 1: Specification of the job content

Specification of the processing

1. Object of processing:

The object of the processing is the provision of a data integration platform („Pipes“).

2. Nature of processing:

The processing shall include possible caching for the duration of the data transfer.

3. Purpose of processing:

The purpose of processing is to connect data sources to a target data store and load data from the data sources into the target data store for centralisation for immediate data access.

Categories of data subjects

The following groups of persons are affected by the job data processing that is carried out:

- Customers
- Users of the pipeline test phase
- Partner
- Contact persons

Types of personal data

The following types of data are affected by the job data processing that is carried out:

- master personal data
- communication data (e.g. telephone, e-mail)
- master contractual data (contractual relationship, product or contractual interest)
- customer history
- contractual settlement and payment data
- planning and control data
- information (from third parties or from public directories)
-

Persons of the Client authorised to issue instructions

The following persons of the Client are entitled to issue instructions to the Contractor:
(please specify name, function and email address)

-
-

Client's data protection officer

The Data Protection Officer of the Client is:
(please specify name, address and email)

…

Persons of the Contractor authorised to receive instructions

The following persons of the Contractor are entitled to receive instructions from the Client:

- Salvatore Raunich/ CTO / salvatore.raunich@datavirtuality.de
- Eugene Bykov/ Connector Development and SaaS Technical Lead / eb@datavirtuality.de

Contractor's data protection officer

The Data Protection Officer of the Contractor is

Marco Tessendorf, procado Consulting, IT & Media Service GmbH

Warsaw Str. 58a
10243 Berlin

Authorised subcontractors

At the time of the conclusion of the contract, subcontractual relations exist with the following subcontractors who provide support services within the framework of the main contract (e.g. data centres):

Name and address of subcontractor	Job content
Amazon Web Services, Inc. (AWS)	Co-location for IT infrastructure and hosting provider

Annex 2: Technical and organisational measures

The technical and organisational measures described below must be treated confidentially. They may not be reproduced in whole or in part or passed on to unauthorised persons.

I. Confidentiality: Physical access checks
The Contractor shall ensure that unauthorised persons do not have access to the office, server and archive rooms. This shall be done by:
• keys/control management • withdrawal of means of access (batch, code card, keys) after expiry of the authorisation • access rules for non-company members, accompaniment of non-company members by personnel • demarcated server room/network distribution (AWS)
II. Confidentiality: Entry controls
The Contractor shall prevent unauthorised persons from using IT systems. This shall be done by:
• password procedures (special characters, minimum length, regular change) • clear assignment of accounts to users, no generic accounts (e.g. Trainee 1, Warehouse, User) • blocking of the user accounts after several failed login attempts • use of firewalls/virus scanner • regular control of the validity of permissions (user accounts) • secure transmission of authentication secrets (credentials) in the network using TLS/HTTPS, SSH, VPN (IPSec, SSL VPN)
III. Confidentiality: Access controls
The Contractor shall warrant that the persons authorised to use a data processing system can only access the data subject to their access authorisation and that personal data are not read, copied, changed or removed without authorisation during processing, use and after storage. This shall be done by:
• binding authorisation process • differentiated authorisations (profiles, roles, transactions and objects) • avoidance of the concentration of functions (separation of functions of administrator activities to different qualified persons) • allocation of minimal authorisations (on a need-to-know basis) • evaluation of accesses and access authorisations
IV. Confidentiality: Separation controls
The Contractor shall warrant that data collected for different purposes can be processed separately. There is no need for physical separation; a logical separation of the data is sufficient. This shall be done by:
• guidelines for the classification of data and documents (public, internal, confidential, strictly confidential) • separation of development, test and operating environments
V. Integrity: Disclosure controls
The Contractual shall warrant that personal data cannot be read, copied, altered or removed without authorisation during electronic transmission or during their transport or storage on data carriers, and that it is possible to check and establish to which points personal data are to be transmitted by data transmission equipment. This shall be done by:

- logging of data transmissions
- encryption/tunnel connections (virtual private network (VPN)) for external access
- arrangements for the use of external storage devices (mobile hard disks, USB sticks, etc.)
- implementation of security gateways (firewalls) at the network transfer points
- presence of security cabinets
- implementation of precautionary measures (destruction of data media, shredder)

VI. Integrity: Input controls

The Contractor shall warrant that it can be subsequently verified and established whether and by whom personal data have been input, modified or removed in data processing systems. This shall be done by:

- central logging and log evaluation systems
- each employee having only the necessary access to the data required within the scope of his or her function/role (principle of minimum rights)
- application-level firewalls and intrusion detection systems being used to prevent and detect attacks

VII. Availability and resilience: Availability controls

The Contractor shall warrant that personal data are protected against accidental destruction or loss. This shall be done by:

- automated standard routines for regular updating of protection software (e.g. virus scanner, malware protection and firewall systems)
- storage systems with redundancy (RAID) are used
- a monitoring concept and permanent system monitoring to detect faults
- backup computer centre (AWS)
- uninterruptible power supply (UPS)

VIII. Availability and resilience: Capacity to be restored

The Contractor shall warrant the ability to rapidly restore the availability of and access to personal data in the event of a physical or technical incident by taking the following measures:

- regular execution of backups
- performance of a regular check of the condition and identification of data carriers for data backups
- separate storage of the backup data media/back-up stocks
- regular, prompt updating of servers and workstations (patch management)

IX. Monitoring, assessment and evaluation

The Contractor shall warrant a process for the regular review and evaluation of the effectiveness of the technical and organisational protective measures. This shall be done by:

- a data protection officer being appointed
- regular security tests (e.g. penetration test) and revisions taking place
- all employees being obliged and instructed in writing to comply with data protection regulations
- the employees entrusted with data processing being familiarised with the regulations on data protection in data protection training courses