Data Processing Agreement – DPA

Preamble

This addendum details the parties' obligations on the protection of personal data, associated with the processing of personal data on behalf of Company as a data controller, in relation to the Company's use of the Supplier's analytical services as described in the Supplier's Terms and Conditions or other written or electronic agreement (hereinafter, the "Agreement"). Its regulations shall apply to any and all activities associated with the Agreement, in whose scope Supplier's employees or agents process Company's personal data (hereinafter, "Data") on behalf of Company as a controller (hereinafter, "Contract Processing").

How to execute this DPA

(1) This DPA consists of two parts: the main body of the DPA, and Exhibits 1 and 2

(2) This DPA has been pre-signed on behalf of the Controller.

(3) To complete this DPA, Company must:

a. Complete their information on page 2

b. Complete their information and sign in the signature section on page 6

(4) Submit the completed and signed DPA to our Data Privacy Officer (DPO) via privacy@test.io

Addendum 1 to the agreement concluded by and between

Company Name: _____

Company Registered Address: _____

hereinafter, “Company”

– and –

test IO GmbH, Sonnenallee 223 a, 12059 Berlin– hereinafter, “Supplier” –

on the processing of personal data on behalf of a controller in accordance with Article 28 (3) of the EU General Data Protection Regulation (GDPR).

§ 1 Scope, duration and specification of contract processing of Data

(1) The scope and duration and the detailed stipulations on the type and purpose of Contract Processing shall be governed by the Agreement. Specifically, Contract Processing shall include, but not be limited to, the Data outlined in Exhibit 1.

(2) Company will not provide (or cause to be provided) any information that falls within the definition of "special categories of data" under EU Data Protection Legislation or any other applicable law relating to privacy and data protection (“Sensitive Data”) to Supplier for Contract Processing, and Supplier will have no liability for Sensitive Data. For the avoidance of doubt, this DPA will not apply to Sensitive Data.

(3) Except where this addendum stipulates obligations beyond the term of the Agreement, the term of this addendum shall be the term of the Agreement.

§ 2 Scope of application and responsibilities

(4) Supplier shall process Data on behalf of Company. Such Contract Processing shall include all activities detailed in the Agreement and its statement of work. Within the scope of this addendum, Company shall be solely responsible for compliance with the applicable statutory requirements on data protection, including, but not limited to, the lawfulness of disclosing Data to Supplier and the lawfulness of having Data processed on behalf of Company. Company shall be the »controller« in accordance with Article 4 no. 7 of the GDPR.

(5) Company’s individual instructions on Contract Processing shall, initially, be as detailed in the Agreement. Company shall, subsequently, be entitled to, in writing or in a machine-readable format (in text form), modifying, amending or replacing such individual instructions by issuing such instructions to the point of contact designated by Supplier. Instructions not foreseen in or covered by the Agreement shall be treated as requests for changes to the statement of work. Company shall, without undue delay, confirm in writing or in text form any instruction issued orally.

§ 3 Supplier’s obligations

(1) Except where expressly permitted by Article 28 (3)(a) of the GDPR, Supplier shall process data subjects’ Data only within the scope of the statement of work and the instructions issued by Company. Where Supplier believes that an instruction would be in breach of applicable law, Supplier shall notify Company of such belief without undue delay. Supplier shall be entitled to suspending performance on such instruction until Company confirms or modifies such instruction.

(2) Supplier shall, within Supplier's scope of responsibility, organize supplier's internal organization so it satisfies the specific requirements of data protection. Supplier shall implement technical and organizational measures to ensure the adequate protection of Company's Data, which measures shall fulfil the requirements of the GDPR and specifically its Article 32. Supplier shall implement technical and organizational measures and safeguards that ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services. Company is familiar with these technical and organizational measures, and it shall be Company's responsibility that such measures ensure a level of security appropriate to the risk.

With regard to compliance with the protective measures and safeguards agreed upon and their verified effectiveness, parties refer to the existing certification issued by WS Datenschutz GmbH presented to and sufficient for Company as proof of the appropriate guarantees, as documented in Exhibit 2 hereto.

Supplier reserves the right to modify the measures and safeguards implemented, provided, however, that the level of security shall not be less protective than initially agreed upon.

(3) Supplier shall support Company, insofar as is agreed upon by the parties, at the expense of Company, and where possible for Supplier, in fulfilling data subjects' requests and claims, as detailed in chapter III of the GDPR and in fulfilling the obligations enumerated in Articles 33 to 36 of the GDPR.

(4) Supplier warrants that all employees involved in Contract Processing of Company's Data and other such persons as may be involved in Contract Processing within Supplier's scope of responsibility shall be prohibited from processing Data outside the scope of the instructions. Furthermore, Supplier warrants that any person entitled to process Data on behalf of Controller has undertaken a commitment to secrecy or is subject to an appropriate statutory obligation to secrecy. All such secrecy obligations shall survive the termination or expiration of such Contract Processing.

(5) Supplier shall notify Company, without undue delay, if Supplier becomes aware of breaches of the protection of personal data within Supplier's scope of responsibility. Supplier shall implement the measures necessary for securing Data and for mitigating potential negative consequences for the data subject; the Supplier shall coordinate such efforts with Company without undue delay.

(6) Supplier shall notify to Company the point of contact for any issues related to data protection arising out of or in connection with the Agreement.

(7) Supplier warrants that Supplier fulfills its obligations under Article 32 (1)(d) of the GDPR to implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

(8) Supplier shall correct or erase Data if so instructed by Company and where covered by the scope of the instructions permissible.

In specific cases designated by Company, such Data shall be stored or handed over. The associated remuneration and protective measures shall be agreed upon separately, unless already agreed upon in the Agreement.

(9) Supplier shall, upon termination of Contract Processing and upon Company's instruction, return all Data, carrier media and other materials to Company or delete the same within 120 days from the date of termination.

Company shall bear any extra cost caused by deviating requirements in returning or deleting data.

(10) Where a data subject asserts any claims against Company in accordance with Article 82 of the GDPR, Supplier shall support Company in defending against such claims, where possible.

§ 4 Company's obligations

(1) Company shall notify Supplier, without undue delay, and comprehensively, of any defect or irregularity with regard to provisions on data protection detected by Company in the results of Supplier's work.

(2) Section 3 para. 10 above shall apply, mutatis mutandis, to claims asserted by data subjects against Supplier in accordance with Article 82 of the GDPR.

(3) Company shall notify to Supplier the point of contact for any issues related to data protection arising out of or in connection with the Agreement.

§ 5 Enquiries by data subjects

Where a data subject asserts claims for rectification, erasure or access against Supplier, and where Supplier is able to correlate the data subject to Company, based on the information provided by the data subject, Supplier shall refer such data subject to Company. Supplier shall forward the data subject's claim to Company without undue delay. Supplier shall support Company, where possible, and based upon Company's instruction insofar as agreed upon. Supplier shall not be liable in cases where Company fails to respond to the data subject's request in total, correctly, or in a timely manner.

§ 6 Options for documentation

(1) Supplier shall document and prove to Company Supplier's compliance with the obligations agreed upon in this addendum by appropriate measures.

Where specific types of documentation and proof can be identified, with regard to compliance with the obligations agreed upon, Supplier may make available to Company internal compliance regulations including external proof of compliance with these regulations.

(2) Where, in individual cases, audits and inspections by Company or an auditor appointed by Company are necessary, such audits and inspections will be conducted during regular business hours, and without interfering with Supplier's operations, upon prior notice, and observing an appropriate notice period. Supplier may also determine that such audits and inspections are subject to prior notice, the observation of an appropriate notice period, and the execution of a confidentiality undertaking protecting the data of other customers and the confidentiality of the technical and organizational measures and safeguards implemented. Supplier shall be entitled to rejecting auditors which are competitors of Supplier.

Company hereby consents to the appointment of an independent external auditor by Supplier, provided that Supplier provides a copy of the audit report to Company.

Supplier shall be entitled to requesting a remuneration for Supplier's support in conducting inspections where such remuneration has been agreed upon in the Agreement. Supplier's time and effort for such inspections shall be limited to one day per calendar year, unless agreed upon otherwise.

(3) Where a data protection supervisory authority or another supervisory authority with statutory competence for Company conducts an inspection, para. 2 above shall apply mutatis mutandis. The execution of a confidentiality undertaking shall not be required if such supervisory authority is subject to professional or statutory confidentiality obligations whose breach is sanctionable under the applicable criminal code.

§ 7 Subcontractors (further processors on behalf of Company)

(1) Supplier shall use subcontractors as further processors on behalf of Company only where approved in advance by Company.

(2) A subcontractor relationship shall be subject to such consent of Supplier commissioning further supplier or subcontractors with the performance agreed upon in the Agreement, in whole or in part. Supplier shall conclude, with such subcontractors, the contractual instruments necessary to ensure an appropriate level of data protection and information security.

Company hereby consents to Supplier's use of subcontractors. Supplier shall maintain an up-to-date list of the names and locations of all subcontractors used for the Contract Processing under the Agreement or this addendum at https://test.io/gdpr and also available upon request to privacy@test.io. Supplier shall update the list on its website at least thirty (30) days prior to the date on which the subcontractor shall commence processing of Data. Company may sign up to receive email notifications of any such changes.

Company shall be entitled to object to any change notified by Supplier within thirty (30) days and for materially important reasons. Where Company fails to contradict such change within such period of time, Company shall be deemed to have consented to such change. Where a materially important reason for such contradiction exists, and failing an amicable resolution of this matter by the parties, Company shall be entitled to terminate the Agreement.

(3) Where Supplier commissions subcontractors, Supplier shall be responsible for ensuring that Supplier's obligations on data protection resulting from the Agreement and this addendum are valid and binding upon subcontractor.

§ 8 Obligations to inform, mandatory written form, choice of law

(1) Where the Data becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while in Supplier's control, Supplier shall notify Company of such action without undue delay unless prohibit from doing so by law. Supplier shall, without undue delay, notify to all pertinent parties in such action, that any data affected thereby is in Company's sole property and area of responsibility, that data is at Company's sole disposition, and that Company is the responsible body in the sense of the GDPR.

(2) No modification of this addendum and/or any of its components – including, but not limited to, Supplier's representations and warranties, if any – shall be valid and binding unless made in writing or in a machine-readable format (in text form), and furthermore only if such modification expressly states that such modification applies to the regulations of this addendum. The foregoing shall also apply to any waiver or modification of this mandatory written form.

(3) In case of any conflict, the data protection regulations of this addendum shall take precedence over the regulations of the Agreement. Where individual regulations of this an addendum are invalid or unenforceable, the validity and enforceability of the other regulations of this addendum shall not be affected.

(4) This addendum is subject to the laws of England and Wales.

§ 9 Liability and damages

Company and Supplier shall be liable to data subject in accordance with Article 82 of the GDPR.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Agreement with effect from the last date of execution below.

Supplier:

Signature: _____

Name: Jan Schwenzien

Title: CEO

Date Signed: _____

Company:

Signature: _____

Name: _____

Title: _____

Date Signed: _____

Exhibit 1 – Details of Contract Processing

This Exhibit 1 includes certain details of the Processing of Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of Company Personal Data

The subject matter and duration of the Processing of the Data are set out in the Agreement.

The types of Company Personal Data to be Processed

• First and last name

• Title

• Position

• Employer

• Contact information (company, email, phone, physical business address)

Categories of data

The personal data transferred concern the following categories of data:

• First and last name

• Title

• Position

• Employer

• Contact information (company, email, phone, physical business address)

• Invoice and transaction history

• Details of the methods of the Data Subject uses to make payments (See Note 1)

• Arbitrary data which the Controller may send to test IO, and which is associated with a Data Subject – (See Note 2)

Notes

(1) This does not include sensitive payment information such as credit card numbers, expiry dates, CVC codes or bank account details.

(2) test IO provides the capability for its customers to associate any data they wish with a Data Subject, utilizing our API. Test IO does not and cannot ascertain what the content or purpose of this data actually is. § 1 (2) stipulates that Company will not provide Sensitive Data.

The obligations and rights of Company

The obligations and rights of Company are set out in the Agreement and this addendum.

Exhibit 2 – Technical and organizational measures acc. Art. 32 Para. 1 GDPR by test IO GmbH, Sonnenallee 223a, 12059 Berlin.

1. Access Control (Premise Level)

Target: to prevent unauthorized persons from gaining access to data processing systems with which personal data are processed or used.

Measures:

- Access solely for authorized employees
- Documented key administration
- Revoking of access rights after expiry of authorization
- Door security
- Security locks

2. Access Control (Computer Level)

Target: to prevent data processing systems from being used without authorization.

Measures:

- Password policy
- Clean Desk Policy obliges every employee to dispose of documents appropriately and to lock their computer when leaving the desk
- Encryption of data storage devices
- Firewall / Virus scanners
- Revoking of access rights after expiry of authorization
- Backup encryption
- Logging and analysis of software incidents being a potential threat
- Technical and organizational actions ensure that authorizations which are not required are being withdrawn in a timely manner

3. Access Control (Authorization Level)

Target: to ensure that persons entitled to use a data processing system have access only to data to which they have a right of access.

Measures:

- Differentiated authorization (e.g. profiles, responsibilities)
- Mechanism for authorizations to enable exact differentiation of level when accessing the backend of software
- Binding authorization process for employees
- Existing administration concept in place ensuring transparent application and distribution of access
- Employee authorizations are documented
- Distribution of minimum access authorizations to employees (Need-to-know)

4. Transmission Control

Target: to ensure that personal data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged.

Measures:

- Secured transfer protocols (SSL, TSL, SFTP)
- The private use of data storage devices at the workplace is not permitted
- Instruction for use of mobile data storage devices
- Process for appropriate deletion / disposal of data storage devices and documents
- Hosting on ISO 27001 certified server centers

5. Input Control

Target: to ensure that it is possible to check and establish whether and by whom personal data have been input into data processing systems, modified or removed.

Measures:

- Access Authorization Concept in Place
- Organizational regulation of authorization of users allowed to make changes is recorded
- Each employee has the appropriate access according to their responsibilities / role
- Distribution of authorizations for employees are distributed by an authorized individual

6. Job Control

Target: to ensure that, in the case of commissioned processing of personal data, the data are processed strictly in accordance with the instructions of the principal.

Measures:

- Control over data processing agreements (DPA)
- DPAs contain detailed information about the appropriation of user of data related to individuals of the contracting authority as well as the prohibition of use of service providers not set in written contract

- The contract contains detailed information of the kind and quantity of the ordered processing and use of data related to individuals of the contracting authority
- The service provider employed a data protection officer and ensures an appropriate integration into relevant organization processes by organization of data protection
- DPAs with all relevant processors are in place
- A clear layout and procedure for issuing DPAs to Controllers is in place
- A security concept is in place
- All employees with access are committed to data security by contract
- Each employee has received work orders and guides informing them on how to apply to actions securing data and ensuring IT security
- The Controller will be notified immediately about a data security breach

7. Availability Control

Target: to ensure that personal data are protected from accidental destruction or loss.

Measures:

- Backup processes / regular security copies
- A fire detection system is in place
- Use of data protection programs and software (e.g. anti-virus protection, firewall)
- Automated standard routines for regular updates of security software
- Automated and permanent monitoring for detection of errors
- Automated workflow for distribution of notifications regarding maintenance and errors

8. Organizational Control

Target: to design the in-house organization in such a way that it meets the requirements of data protection.

Measures:

- All employees are informed about and legally committed to data security and privacy
- All employees are issued with work instructions on data privacy
- All employees are regularly trained on data privacy at the workplace
- A regular audit carried out by the commissioner of date security
- A clear regulation of representative within groups is in place
- A procedure for regular tests, analysis and evaluation acc. Art. 32 Para. 1 GDPR is in place

Data Privacy by Design acc. Art. 25 Para. 2 GDPR is realized according to these technical and organizational measures.