

## Data Processing Addendum

### in accordance with Article 28 General Data Protection Regulation (GDPR)

This Data Processing Addendum (the "Addendum") is made and entered into by and between Desk-Net GmbH ("Processor") and the customer specified in the table below ("Controller"). This Addendum covers all issues of data protection between the Processor and Controller.

Hamburg, 17.05.2018   _____	City and Date: _____  _____
Signatory: <b>Matthias KRETSCHMER</b>	Signatory: _____
Title: <b>CEO</b>	Title: _____
Company Name: <b>Desk-Net GmbH</b>	Company Name (Required): _____
Address:  Hoheluftchausee 21, 20253 Hamburg, Germany	Address: _____ _____

This Addendum includes the data processing terms and Technical and Organisational Measure ("TOMs") and supplements the Master Agreement between Controller and Processor which governs the Controller's use of the software Desk-Net ("Master Agreement"). This Addendum will be effective as of the day Desk-Net receives a complete and executed Addendum from the Controller.

#### 1. Addendum Subject Matter and Duration

- 1) The Subject matter of this Addendum results from the Desk-Net Master Agreement, hereinafter referred to as Master Agreement.
- 2) The duration of this Addendum corresponds to the duration of the Master Agreement.

## **2. Addendum Specification**

### 1) Nature and purpose of the intended processing of data:

The Nature and Purpose of the data processed is subject to the services provided by the Processor: Operation of the web application Desk-Net for story planning, staff coordination and task management.

### 2) Type of Data

The following data types are subject of the processing of personal data:

- Person related Master Data (Key Personal Data)
- Contact Data (Telephone, Email)
- Planning and Control Data
- Other: Shift assignment

### 3) Categories of data subjects

The Categories of data subjects (Users in the sense of the Master Agreement) comprises:

- Controller's Employees
- Controller's Suppliers

### 4) Location of the data Processing

The undertaking of the contractually agreed Data Processing 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 data is exclusively hosted in the EU at Amazon Web Services in Dublin, Republic of Ireland.

## **3. Technical and Organisational Measures**

- 1) Before the commencement of processing, the Processor shall make available to the Controller the documented Technical and Organisational Measures for inspection. Upon acceptance by the Controller, the documented measures become the foundation of the agreement. Insofar as the inspection/audit by the Controller shows the need for amendments, such amendments shall be implemented by mutual agreement.
- 2) The Processor shall establish the 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. The measures to be taken are measures of data security and measures that guarantee 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 probability of occurrence

and the severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 Paragraph 1 GDPR must be taken into account.

- 3) The 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 so doing, the security level of the defined measures must not be reduced. Substantial changes must be documented.

#### **4. Rectification, Restriction and Erasure of Data**

- 1) The Processor may not on its own authority rectify, erase or restrict the processing of data that is being processed on behalf of the Controller, but only on documented instructions from the Controller.

Insofar as a User contacts the Processor directly concerning a rectification, erasure, or restriction of processing, the Processor will immediately forward the User's request to the Controller.

- 2) Insofar as it is included in the scope of services, the erasure policy, 'right to be forgotten', rectification, data portability and access shall be ensured by the Processor in accordance with documented instructions from the Controller without undue delay.

#### **5. Quality assurance and other duties of the Processor**

In addition to complying with the rules set out in this Addendum, the Processor shall comply with the statutory requirements referred to in Articles 28 to 33 GDPR; accordingly, the Processor ensures, in particular, compliance with the following requirements:

- a) Written appointment of a Data Protection Officer. Ms. Claire Scott, +49 40 88 14 170 0, [dpo@desk-net.com](mailto:dpo@desk-net.com) is designated as the DPO on behalf of the Processor. Any changes on this matter shall be communicated to the Controller.
- b) 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 contract who have been bound to confidentiality and have previously been familiarised with the data protection provisions relevant to their work. The Processor and any person acting under its authority who has access to personal data, shall not process that data unless on instructions from the Controller, which includes the powers granted in this contract, unless required to do so by law.
- c) Implementation of and compliance with all Technical and Organisational Measures necessary to this Addendum in accordance with Article 28 Paragraph 3 Sentence 2 Point c, Article 32 GDPR.

- d) The Controller and the Processor shall cooperate, upon request, with the supervisory authority in performance of its tasks.
- e) The Controller shall be informed immediately of any inspections and measures conducted by the supervisory authority, insofar as they relate to this Addendum. 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 the processing of this Addendum.
- f) 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 in connection with the data processing by the Processor, the Processor shall make every effort to support the Controller.
- g) The Processor shall periodically monitor the internal processes and the Technical and Organizational Measures to ensure that processing within his area of responsibility is in accordance with the requirements of applicable data protection law and the protection of the rights of the data subject.
- h) Verifiability of the Technical and Organisational Measures conducted by the Controller as part of the Controller's supervisory powers referred to in Section 7 hereto.

## **6. Subcontracting**

- 1) For the purpose of this Addendum Subcontracting is to be understood as meaning only services which relate directly to the provision of the main service as set out in Section 2(1) hereto. This does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support 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 equipment. The Processor shall, however, be obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the protection and security of the Controller's data, even in the case of outsourced ancillary services.
- 2) The Processor may replace or add subcontractors (further processors) insofar as:
  - a) The Processor informs the Controller in writing of such subcontracting reasonably in advance,
  - b) The Controller does not object to the addition or replacement of the subcontractor in writing or text form before the planned replacement or addition,

c) an agreement in accordance with Art. 28 para. 2-4 GDPR is used

3) The Controller agrees to the commissioning of the following subcontractors in the condition of a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR:

Subcontracted Company	Address / Country	Service provided
Intetics GmbH Sp. z o.o.	ul. Marii Skłodowskiej-Curie 5/5 31-025 Krakaw, Poland	Operation and maintenance of the Desk-Net application
Amazon Web Services EMEA SARL (AWS Europe)	38 avenue John F. Kennedy L-1855 Luxembourg	Hosting of the Desk-Net and Backup (only on servers inside the EU)

4) The transfer of personal data from the Controller to the subcontractor and the subcontractors' commencement of the data processing shall only be undertaken after compliance with all requirements has been achieved.

5) 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 to ancillary service providers in accordance with this Section 6 (1).

## **7. 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. Controller has the right to convince itself of the Processor business operations compliance with this agreement by means of random checks, which are ordinarily to be announced in a reasonable time.

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

3) Evidence of such measures, which do not only concern this specific agreement, may be provided by:

a) Compliance with approved Codes of Conduct pursuant to Article 40 GDPR;

- b) Certification according to an approved certification procedure in accordance with Article 42 GDPR;
  - c) 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)
  - d) A suitable certification by IT security or data protection auditing (e.g. according to BSI-Grundschutz (IT Baseline Protection certification developed by the German Federal Office for Security in Information Technology (BSI)) or ISO/IEC 27001).
- 4) The Processor may claim remuneration for enabling Controller inspections.

## **8. Communication in the case of infringements by the Processor**

- 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, referred to in Articles 32 to 36 of the GDPR. These include:
  - a) Ensuring an appropriate level of protection through Technical and Organizational Measures that take into account the circumstances and purposes of the processing as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events.
  - b) The obligation to report a personal data breach immediately to the Controller
  - c) The duty to assist the Controller with regard to the Controller's obligation to provide information to the Data Subject concerned and to immediately provide the Controller with all relevant information in this regard.
  - d) Supporting the Controller with its data protection impact assessment
  - e) Supporting the Controller with regard to prior consultation of the supervisory authority
- 2) The Processor may claim compensation 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. Authority of the Controller to issue instructions**

- 1) The Controller shall immediately confirm oral instructions (at the minimum in text form).
- 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.

## **10. 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 Master 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 contract 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 upon request.
- 3) Documentation which is used to demonstrate orderly data processing in accordance with the Contract shall be stored beyond the contract duration 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.