Commissioned Data Processing Agreement according to Art. 28 GDPR

between

Expocloud GmbH
Eupener Straße 332
52076 Aachen

- hereinafter referred to as `Principal´ -

and

_____ **(company name)**

_____ **(Adress)**

_____ **(Postcode & City)**

- hereinafter referred to as `Agent´ -

1. Subject-matter and duration of the agreement

(1) subject-matter of the agreement

☒ The subject of the agreement results from the ordered software subscriptions and their service descriptions (in the respective current version).

oder

☐ The subject-matter of the data processing agreement is the performance of the following tasks by the Agent: ……

(2) duration

☐ The duration (term) of this agreement is equal to the term of the Service Agreement.

or *(particularly where there is no Service Agreement for a specified term)*

☐ The agreement is valid for a one-off task.

☐ The duration (term) of this agreement runs until .....

☒ The agreement is given for an indefinite period of time and may be terminated by either party with a period of notice of 6 weeks. The possibility of termination without notice remains unaffected.

2. Details of the substance of the agreement

(1) Scope, nature and purpose of the proposed collection, processing or use of data

☒ The scope, nature and purpose of the collection, processing and/or use of personal data by the Agent on behalf of the principal are described in detail in the Service Agreement, which is freely accessible online in its latest version.

or

☐ More detailed description of the subject-matter of the agreement in terms of the scope, nature and purpose of the tasks to be carried out by the Agent: .....

The data will be processed and used exclusively within the territory of the Federal Republic of Germany, a Member State of the European Union or another signatory to the Agreement on the European Economic Area. Any movement of data to a third country is subject to compliance with the special requirements set out in Articles 44ff GDPR. The adequate level of protection

☐ is established by a decision of the European Commission on adequacy (Art. 45 para. 3 GDPR);

☒ is ensured by mandatory internal data protection rules (Art. 46 para. 2 GDPR);

☐ is ensured by standard contractual clauses under Directive 95/46/EC of the European Parliament and of the Council (Art. 46 para. 2 GDPR);

☐ is ensured by approved rules of conduct (Art 46 para. 2 GDPR);

☐ is ensured by an approved certification mechanism (Art. 46 para. 2 and Art. 42 GDPR).

☐ is ensured by additional measures: …… (Art. 46 para. 2f GDPR)

(2) Nature of the data

☐ The nature of the personal data to be used is described in detail in the Service Agreement under: .....

or

☒ The subject-matter of the collection, processing and/or use of personal data covers the following types/categories of data (list/description of categories of data)

☒ Person master data

☒ Communication data (eg. Phone number, E-Mail)

☒ Contract master data (contractual relationship, product or contractual interest)

☒ Customer history

☒ Billing and payment data

☒ Planning and management data

(3) Persons affected (data subjects)

☐ The group of data subjects affected by the processing of their personal data within this agreement is described in detail in the Service Agreement under: .....

or

☒ The group of data subjects affected by the processing of their personal data within this agreement includes:

- ☒ Customers
- ☒ Prospects
- ☒ Subscribers
- ☒ Employees
- ☒ Suppliers
- ☒ Commercial representatives
- ☒ Contacts

The processing concerns all users registered in the Expocloud Portal.

3. Technical and organizational measures (Enclosure 1)

(1) The Agent must document the implementation of the technical and organizational measures stipulated in advance of the agreement before starting to process the data, giving details of the actual process to be followed, and must present this to the Principal for review. When accepted by the Principal, the documented measures will form the basis of the agreement. Where this review or an audit by the Principal raises the need for amendments, these must be applied amicably.

(2) Overall, the measures to be taken include actions not specific to the agreement in relation to organizational control, access control, disclosure control, input control, job control and availability control, and to the need for a segregation of functions (see Annex ...), and agreement-specific actions (particularly with regard to the type of data transfer/provision of data, the nature/method of data processing/storage and the nature/method of output/dispatch of the data), described separately below – where these are not covered by the underlying Service Agreement.

(3) The technical and organizational measures are subject to technical progress and development, and the Agent may implement adequate alternative measures. These must not however fall short of the level of security provided by the specified measures. Any material changes must be documented.

4. Correction, restriction and deletion of data

The Agent may only correct, delete or block the data processed on behalf of the Principal when instructed to do so by the Principal. If a data subject should apply directly to the Agent to request the correction or deletion of his personal data, the Agent must forward this request to the Principal without delay.

5. Controls and other responsibilities of the Agent

In addition to complying with the provisions of this agreement, the Agent has the following responsibilities under articles 28 to 33 GDPR:

a) ☐ Written appointment of a data protection officer, able to discharge his duties as set out in Sections 4f and 4g BDSG. The official's contact details must be supplied to the Principal to enable direct contact to be made.

☐ The Agents Data protection officer is:

_____

The Prinicipal must be informed immediately of any change of the data protection officer.

☐ Their current contact details are easily accessible on the Agent's homepage.

b) ☒ The Agent is not obliged to appoint a data protection officer. Dr. Christian Coppeneur-Gülz, 0049 2472 991055, Christian.coppeneur-guelz@expocloud.com is named as the contact person at the Agent.

c) ☐ Since the Agent is based outside the Union, it shall appoint the following representative in the Union in accordance with Article 27(1) of the GDPR: [Add: Firstname, Lastname, Organizational Unit, Phone number, E-Mail].

d) The maintenance of confidentiality in accordance with Section 5 BDSG. All persons who have access to personal data belonging to the Principal under the terms of this agreement must give an undertaking to maintain confidentiality and must be informed of any special data protection requirements arising from this agreement, and the limitation of use to specific purposes as instructed.

e) The implementation of and compliance with all technical and organisational measures required for this contract in accordance with Art. 28 para. 3 sentence 2 lit. c, 32 GDPR [details in Enclosure 1].

f) The contracting authority and the Agent shall cooperate with the supervisory authority on request in the performance of its tasks.

g) The immediate information of the contracting authority on control actions and measures of the supervisory authority, insofar as they relate to this contract. This shall also apply where a competent authority, in the course of administrative or criminal proceedings, investigates the processing of personal data relating to the processing of the contract at the Agent's premises.

h) Monitoring of the agreement by way of regular reviews by the Agent concerning the performance and fulfillment of the contract, particularly compliance with and any necessary amendment to provisions and measures laid down to carry out the agreement.

i) Evidence to be provided to the Principal of the technical and organizational measures taken. For this purpose, the Agent may present up-to-date attestations, reports or extracts thereof from independent bodies (e.g. external auditors, internal audit, the data protection officer, the IT security department or quality auditors) or suitable certification by way of an IT security or data protection audit (e.g. 'IT basic security' as defined by the Federal Office for Information Security - BSI).

6. Subagreements (Enclosure 2)

(1) For the purposes of this provision, subcontracting relationships are understood to be those services which are directly related to the provision of the main service. This does not include ancillary services which the Agent uses, for example, as telecommunications services, postal/transport services, maintenance and user service or the disposal of data carriers, or other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. The Agent is, however, obliged to take appropriate and legally compliant contractual agreements and control measures to ensure data protection and data security of the Customer's data even in the case of outsourced ancillary services.

(2) The agreementing of sub-contractors is only permitted with the prior written consent of the Principal. The Agent may engage his own affiliated companies or other sub-contractors for the performance of the contract without written consent, if he exercises the due care required by law, complies with the monitoring obligation set out in point (5) above, and informs the Principal before starting to process or use the data.

a) ☐ Subcontracting is not permitted.
b) ☒ The Principal agrees to the commissioning of the subcontractors named in Enclosure 2 under the condition of a contractual agreement in accordance with Art. 28 para. 2-4 GDPR.
c) ☒ Outsourcing to subcontractors or

☒ the change of existing subcontractors is valid, provided that:

- the Agent notifies the Principal of such outsourcing to subcontractors in text form a reasonable time in advance, and
- the Principal does not protest to the Agent in text form against the planned outsourcing by the time the data is handed over, and
- it is based on a contractual agreement in accordance with Article 28 of the GDPR

(3) The passing on of personal data of the Principal to the subcontractor and its first action are only permitted when all requirements for a subcontracting have been met.
(4) If the subcontractor provides the agreed service outside the EU/EEA, the Agent shall ensure that it is permissible under data protection law by taking appropriate measures. The same applies if service providers within the meaning of Paragraph 1 Sentence 2 are to be used.
(5) A further outsourcing by the subcontractor

☐ is not permitted;
☐ requires the express consent of the Principal (at least text form);
☒ requires the express consent of the Agent (at least text form);

All contractual regulations in the contractual chain must also be imposed on the further subcontractor.

7. Monitoring rights of the Principal

The Principal may carry out the job control stipulated in No. 6 of the Annex to Section 9 BDSG in consultation with the Agent or appoint auditors to do so. The Principal may carry out sample checks on the Agent's business premises, generally to be announced in advance, in order to verify compliance with this Agreement by the Agent. The Agent undertakes to provide the Principal with the information required to meet his job control obligation and make the necessary documentation available.
Regarding the monitoring obligations of the Principal under Section 11 sentence 4 BDSG before the start of data processing and throughout the term of the agreement, the Agent must ensure that the Principal can confirm adherence to the technical and organizational measures taken. For this purpose, the Agent must provide the Principal upon request with evidence of the implementation of the technical and organizational measures pursuant to Section 9 BDSG and the Annex thereto. Evidence of the implementation of any measures that do not only affect the specific agreement may also be presented in the form of up-to-date attestations, reports or extracts thereof from independent bodies (e.g. external auditors, internal audit, the data protection officer, the IT security department or quality auditors) or suitable certification by way of an IT security or data protection audit (e.g. 'IT basic security' as defined by the Federal Office for Information Security - BSI).

8. Notification of infringements by the Agent

The Agent must notify the Principal in all cases where the Agent or persons employed by him infringe provisions relating to the protection of personal data belonging to the Principal or any other stipulations set out in the agreement.

The Parties are aware that Section 42a BDSG may impose a duty to inform in the event of the loss or unlawful disclosure of personal data or access to it. Such incidents should therefore be notified to the Principal immediately, regardless of their origin. This also applies to serious operational faults or where there is any suspicion of an infringement of provisions relating to the protection of personal data or other irregularities in the handling of personal data belonging to the Principal. In consultation with the Principal, the Agent must take appropriate measures to secure the data and limit any possible detrimental effect on the data subjects. Where obligations are placed in the Principal under Section 42a BDSG, the Agent must assist in meeting them.

9. Principal's authority to issue instructions

(1) Verbal instructions shall be confirmed by the Principal immediately (at least in text form).

(2) The Agent must inform the Principal immediately if he believes that an instruction violates data protection regulations. The Agent is entitled to suspend the execution of the relevant instruction until it is confirmed or amended by the Principal.

10. Deletion of data and return of data media

(1) Copies or duplicates of the data will not be made without the knowledge of the Principal. Excluded from this are back-up copies, insofar as they are necessary to ensure proper data processing, as well as data which is required in order to comply with statutory storage obligations.

(2) Upon completion of the contractually agreed work or earlier upon request by the Principal - at the latest upon termination of the service agreement - the Agent shall hand over to the Principal all documents, processing and usage results and data stocks that have come into its possession and are related to the contractual relationship, or destroy them in accordance with data protection laws upon prior consent. The same applies to test and reject material. The protocol of the deletion must be presented on request.

(3) Documentation which serves as proof of the orderly and proper data processing shall be kept by the Agent in accordance with the respective retention periods beyond the end of the contract. He can hand them over to the customer at the end of the contract to relieve him of this burden.

On behalf of the Principal:	**On behalf of the Agent:**
Name und position:	Dr. Christian Coppeneur-Gülz, CEO:
_____	
Place, Date, Signature:	Place, Date, Signature:
_____	Aachen, 21.01.2020

Enclosure 1 - Technical-organisational measures

1. Confidentiality (Art. 32 para. 1 lit. b GDPR)

Access control

- Access to the building in Monschau is only possible during working hours between 08.00 and 18.00 hours. If required, the keys can be retrieved after entry in a list of selected employees.
- Access to the server room in Monschau is controlled by issuing and logging the key. This is the responsibility of the management and must be collected if necessary.
- Customers and visitors receive a visitor pass at the reception desk.
- The company premises are monitored by video.

Entry control

- Access to the systems is only possible for authorized users. Authorisation is provided by secure passwords (min. eight digits long and consisting of letters, numbers and special characters) and Microsoft's two-factor authentication.
- Antivirus software is active on each device
- After 15 minutes of inactivity by the user, the screen is automatically locked. The lock must be activated manually when the user leaves the work station.
- A hard disk encryption has been set up on the systems.
- WWM's internal network is protected by a firewall at all locations. The sites are connected with an encrypted Site-To-Site-VPN connection.

Access control

- Access to personal data is only granted by authorised users, and the relevant authorisations are granted on the basis of Active Directory.
- The assignment of rights is possible for a maximum of three system administrators.
- Data records can only be read, copied, changed or removed by the intended users.
- The copying of personal data to external data carriers is not permitted.
- Each workstation is equipped with a lockable roller container in which all documents and devices are to be included after the end of work.
- The remote access for remote administration of the devices is encrypted via TLS with a 2048-bit RSA key.

Separation Control

- All project-relevant data is stored depending on the myWWM contract code and is only available for analyses according to the specifications of the responsible person.

Pseudonymisation

- The appropriate processing takes place internally via uniquely assigned identification numbers. A personal reference cannot be read directly from the system.
- A personal reference to a data record is not created until the order is fulfilled.

2. Integrity (Art. 32 para. 1 lit. b GDPR)

- handover control
  The data is processed in Microsoft Dynamics NAV. The software controls the integrity of the data records and offers an integrity check function.
  The transfer of data between the customer's browser and the system on which processing takes place is protected by an SSL certificate with hybrid encryption.
- Input control
  The certified ERP system Microsoft NAV has a logging of changes to personal data. The content before and after the change, as well as the responsible employee and the time are logged.
  The log data is stored for 3 years.

3. availability and resilience (Art. 32 para. 1 lit. b GDPR)

- availability control

  Central backup servers are available for storing backup data. The RAID-1 disk system reduces the likelihood of data loss.
  All backups are additionally backed up in Microsoft Azure.
  The uninterruptible power supply (UPS) is guaranteed by a 15-minute battery capacity. All UPS systems are designed redundantly.
  The servers are continuously provided with security updates.
  Direct free cooling ensures environmentally friendly cooling of the IT hardware. Air conditioning is via the raised floor.

4. procedure for regular review, evaluation and evaluation (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

- incident response management
  - Monitoring of data adjustments
  - Camera surveillance of the company premises
- Data protection-friendly default settings (Art. 25 para. 2 GDPR)
  - Manual deletion according to legal requirements
  - Manual deletion on request
- order control
  - Selection of a contractor from the point of view of due diligence (regarding data security)
  - Agent has appointed data protection officer
  - Obligation of the Agent’s employees to observe data secrecy

Enclosure 2: Subagreements

1 Microsoft Deutschland GmbH

1.1 Company

Microsoft Deutschland GmbH
Walter-Gropius-Straße 5
80807 München
Deutschland

1.2 Services

Hosting

1.3 Processing Agreement (GDPR §28)

30.8.2018

2 Hubspot GmbH

2.1 Company

Hubspot GmbH
Unter den Linden 26
10117 Berlin
Deutschland

2.2 Services

CRM-Software
Ticket-System

2.3 Processing Agreement (GDPR §28)

25.5.2018

3 aConTech Enterprise IT-Solutions GmbH

3.1 Company

aConTech Enterprise IT-Solutions GmbH
Mohnweg 9
90768 Fürth
Deutschland

3.2 Services

IT-Support

3.3 Processing Agreement (GDPR §28)

30.08.2018