Agreement on Order (Data) Processing

between

the FUMO Solutions customer, hereinafter referred to as the "**Customer**"

and

FUMO Solutions GmbH
Lerchenbergstraße 27
89160 Dornstadt

- The processor as defined by Article 24 of the GDPR,
hereinafter referred to as the "**Contractor**"

As at 15.05.2018

1. Subject and duration of the order

1.1 The purpose of the order for the processing of personal data is for the Contractor to perform the tasks in accordance with the contract concluded between the parties ("main contract"). The contract has come about as a result of the registration process of the modules concerned and any future modules.

1.2 The duration of the order corresponds to the duration of the contract, which has come about as a result of the registration process of the modules concerned and any future modules.

2. Specification of the content of the order

2.1 The nature and purpose of the Contractor's tasks are derived from the main contract.

2.2 The data processing in the order only takes place in a member state of the European Union or another country which is a signatory to the Agreement on the European Economic Area. Any transfer to a third country requires the Customer's prior written consent and may only take place if the special requirements of Article 44 et seq. of the GDPR[1] are met.

2.3 The subject matter of personal data processing covers the following types of personal data:

- Personal master data
- Communication data (e.g. telephone, e-mail)
- Contract master data (contractual relationship, product or contractual interest)

[1] §§ 4b, 4c of the BDSG, version up to 25.05.2018.

- Customer history
- Contract billing and payment data
- Planning and control data
- Information (from third parties such as credit agencies or from public directories)
- Employee driving data such as categories of driving licence, driving times, vehicles driven and contracts

2.4 The categories of data subjects involved in this contract include:

- Customers
- Interested parties
- Subscribers
- Employees
- Suppliers
- Commercial agents

3. Technical and organisational measures

3.1 The Contractor must document the implementation of the technical and organisational measures presented prior to the order placement before the processing starts (particularly with regard to the actual implementation of the order), and deliver them to the Customer for review. If accepted by the Customer, the documented measures will become the basis of the order. Any adjustment requirements that may arise as a result of the Customer carrying out the review must be implemented by mutual agreement.

3.2 The Customer shall take the required measures in accordance with Articles 25 and 32 of the GDPR[2] and shall ensure that personal data is lawfully processed in accordance with Article 5 of the GDPR[3]. Overall, the measure to be taken are data security measures and ensure a level of protection appropriate to the level of risk in terms of system confidentiality, integrity, availability and capacity. State-of-the-art technology, implementation costs and the type, scope and purpose of the processing, as well as the differing probability of occurrence and severity of the risk for the rights and freedoms of natural persons must be taken into account in accordance with Article 32 (1) of the GDPR (see **Annex**).

3.3 The technical and organisational measures are subject to technical progress and further development. In this respect, the Contractor is permitted to implement alternative and appropriate measures. The safety level of any specified measures must not in any way be compromised. Significant changes must be documented.

4. Correction, restriction of processing and deletion of data

[2] § 9 of the BDSG and annex to § 9 (1) of the BDSG, version up to 25.05.2018.
[3] § 4 of the BDSG, version up to 25.05.2018.

4.1 The Contractor shall only correct or delete the data processed in the order or restrict the processing of the data after receiving documented instructions from the Customer. If a data subject contacts the Contractor directly for the purpose of correcting or deleting the data subject's data, the Contractor will immediately forward this request to the Customer.

4.2 Insofar as this is included in the main contract, deletion, right to be forgotten, correction, data portability and information are to be ensured by the Contractor in accordance with the Customer's documented instructions.

5. Quality assurance and other obligations of the Contractor

In addition to complying with the provisions of this order, the Contractor has the following obligations in accordance with Articles 28 to 33 of the GDPR[4], in particular:

- Arranging the written appointment of a data protection officer who can carry out his/her activity in accordance with Articles 38 and 39 of the GDPR[5]. The Customer will be notified of the contact details of the data protection officer. This will allow the Customer to make direct contact with the data protection officer concerned. The Customer will be immediately notified if there is a change of data protection officer.

- Maintaining confidentiality in accordance with Article 32 Section 4[6] of the GDPR. Any persons authorised to access the Customer's personal data in accordance with the order must first be required to maintain confidentiality and have been informed about the relevant data protection requirements. The Contractor, and any person working for the Contractor who has access to personal data within the scope of the order, may process this data in accordance with Article 29 of the GDPR only on the Customer's instructions, unless they are required to process the data in accordance with the laws of the European Union or the law of the members states.

- Ensuring implementation and compliance with all technical and organisational measures required for this order in accordance with Articles 25 and 32 of the GDPR[7] and the **annex** to this agreement.

- On request, and together with the Customer, collaborating with the supervisory authority in carrying its duties.

- Notifying Customer immediately about the supervisory authority's inspection activities and measures in regard to the order. This also applies if a competent

[4] § 11 (4) of the BDSG, version up to 25.05.2018.
[5] §§ 4f, 4g of the BDSG.
[6] § 5 of the BDSG, version up to 25.05.2018.
[7] § 9 of the BDSG and annex to § 9 (1) of the BDSG, version up to 25.05.2018.

authority carries out an investigation at the Contractor's premises as part of non-compliance or criminal proceedings.

- Doing its utmost to assist the Customer in the event of the Customer being subject to any inspection by the supervisory authority, non-compliance or criminal proceedings, liability claim of a data subject or a third party or any other claim relating to the Contractor's order processing.

- Using regular checks to carry out order control in regard to the execution and fulfilment of the contract. This relates, in particular, to compliance with and any necessary adaptation of rules and measures for carrying out the order to ensure that processing by the Contractor is conducted lawfully and the rights of the data subject are protected.

- Collecting evidence of technical and organisational measures taken that can be shown to the Customer. The Contractor may also provide up-to-date certificates, reports or extracts from reports from independent bodies (e.g. accountants, auditors, data protection officers, IT security departments, privacy auditors, quality auditors) or appropriate certification by an IT security or data protection audit (e.g. in accordance with the BSI Grundschutz).

6. Subcontracting

6.1 If subcontractors (other order processors as defined by Article 28 of the GDPR) are to be included in the processing or use of the Customer's personal data, this will be approved if the following conditions are met:

- Involvement of subcontractors is generally only permitted with the Customer's written consent (a fax or e-mail will suffice). Without such consent, the Contractor may use subcontractors with statutory due diligence to carry out the contract, subject to the order control requirement set out in section 5, if the Contractor notifies the Customer of this prior to the start of the processing or use in writing, and the Customer has not objected to the relocation of the data processing within one month of the receipt of the notification in writing.

- The Contractor must draw up the contractual agreements with the subcontractor in such a way that they comply with the data protection provisions in the contractual relationship between the Customer and the Contractor, as well as Article 28 of the GDPR.

- In the case of subcontracting, the Customer must be granted monitoring and inspecting rights in accordance with this Agreement. This also includes the right of the Customer to obtain from the Contractor on written request information about the key content of the contract and the enforcement of data pro-

tection requirements in the subcontractual relationship, if necessary by inspection of the relevant contractual documents.

- The involvement of the subcontractor is not permitted unless all the above conditions are met.

- The aforementioned conditions shall also apply if the subcontractor wishes to set up its own subcontracting relationship.

- The Contractor has already authorised the involvement of the following subcontractors:

  1&1 Internet SE, Elgendorfer Str. 57, 56410 Montabaur (DE)
  Hosting the web platform

  Microsoft Cooperation, One Microsoft Way, Redmond, WA 98052-6399 (USA)
  E-mail communication using Office 365

6.2 For the purpose of this regulation, these services that the Contractor uses as ancillary services from third parties to assist in the execution of the order should not be understood as subcontracting relationships. These include, for example, telecommunication services, maintenance and user services, cleaners, auditors and disposal of data carriers. However, the Contractor is required to make appropriate and legally compliant contractual agreements and to take control measures to ensure the protection and security of the Customer's data, even where use is made of outsourced ancillary services.

6.3 If the subcontractor does not provide its services in a member state of the European Union or in any other country that is a signatory to the Agreement on the European Economic Area, or if this is the case with a service provider used by the subcontractor in accordance with paragraph 6.2, the Contractor shall ensure that the processing of personal data is lawful.[8]

7. Inspection rights of the Customer

7.1 The Customer has the right to carry out inspections in consultation with the Contractor or to have such inspections carried out by a designated inspector in specific cases. The Customer has the right to carry out spot checks which should be notified to the Contractor in good time to ensure that the Contractor complies with this Agreement in respect to its business operations. On request, the Contractor agrees to provide the Customer with the information required to comply with the Contractor's obligations under Article 28 of the GDPR[9] and to provide appropriate evidence.

[8] Subcontracting with service providers in third countries is only possible from 25.05.2018 as order data processing. Until this date this can only be done using the standard contractual clauses.

[9] No. 6 of the annex to § 9 (1) of the BDSG, version up to 25.05.2018.

7.2 In regard to the Customer's inspection obligations prior to the start of data processing and during the term of the order, the Contractor shall ensure that the Customer is satisfied in terms of compliance with technical and organisational measures taken. Accordingly, the Contractor will inform the Customer on request of the implementation of the technical and organisational measures in accordance with Articles 25 and 32 of the GDPR[10] and the **annex**. The evidence of the implementation of these measures, which do not only concern the actual contract, can also be provided by presenting up-to-date certification, reports or extracts from reports of independent bodies (e.g. accountants, auditors, data protection officers, IT security departments, data protection auditors, quality auditors) or suitable certification by an IT security or data protection audit (e.g. in accordance with BSI Grundschutz) or compliance with approved codes of conduct in accordance with Article 40 of the GDPR or certification in accordance with an approved certification procedure pursuant to Article 42 of the GDPR[11].

8. Notification in the event of violations by the Contractor

8.1 The Contractor shall in all cases submit a report to the Customer if the Customer or the persons employed by the Customer have violated regulations governing the protection of the Customer's personal data or have violated the provisions made in the contract.

8.2 The Contractor shall assist the Customer in meeting the Customer's obligations in accordance with Article 32 et seq. of the GDPR by

- Ensuring adequate levels of protection by putting in place technical and organisational measures that take into account the circumstances and purposes of the processing, as well as the predicted likelihood and severity of a possible infringement of rights by security loopholes, and enable the immediate detection of relevant events.

- Meeting the requirement to report violations of personal data immediately to the Customer.

- Meeting the requirement to assist the Customer in providing information to the data subject and to provide the Customer with any relevant information without delay in this regard.

- Assisting the Customer with their privacy impact assessment.

- Assisting the Customer with prior consultations with the supervisory authority.

9. Authorisation of the Customer

[10] § 9 and annex to § 9 (1) of the BDSG, version upt to. 25.05.2018.
[11] Only relevant from 25.05.2018.

9.1 The handling of the data takes place only within the framework of the agreements made and in accordance with the Customer's instructions (cf. Article 29 of the GDPR[12]). Within the framework of the order description made in this Agreement, the Customer reserves a comprehensive right to issue instructions regarding the type, scope and procedure of the data processing, which the Customer may substantiate by issuing individual instructions. Changes to the subject matter of the processing and procedural changes must be agreed and documented on a joint basis. The Contractor may only give information to third parties or the data subject with the Customer's prior written consent.

9.2 Verbal instructions will be confirmed by the Customer immediately in writing (a fax or e-mail will suffice). The Contractor shall not use the data for any other purposes and, in particular, is not entitled to pass data on to third parties. Copies and duplicates shall not be made without the Customer's prior knowledge. This does not include back-up copies – if these are required to ensure that data processing is carried out in the proper manner – and data required to comply with statutory retention requirements.

9.3 The Contractor must inform the Customer immediately if the Contractor believes that an instruction violates statutory data protection regulations. The Contractor shall be entitled to defer the execution of the relevant instruction until the instruction has been confirmed or modified by the person responsible at the Customer's business.

10. Deletion of data and return of data carriers

10.1 The Contractor is not entitled to make copies of personal data. This does not include back-up copies - if these are required to ensure that data processing is carried out in the proper manner – and data required to comply with statutory retention requirements.

10.2 After the contractual work has been concluded or at any earlier date requested by the Customer – but no later than the date on which the service agreement ends – the Contractor shall deliver to the Customer all documentation, any results derived from the processing and usage of data, as well as data files that are relevant to the contractual relationship, or destroy them in accordance with data protection law. The same applies to test and scrap material. The evidence of such deletion must be submitted on request.

10.2 Documentation serving as proof of order-related and proper data processing must be kept by the Contractor beyond the end of the contract in accordance with respective retention periods. The Contractor may deliver them to the Customer for safekeeping at the end of the contract.

[12] § 11 (3) (1) of the BDSG, version up to 25.05.2018.

11. Final provisions

11.1 This contract supplements the order, which has come about as a result of the registration process of the modules concerned and any future modules. There are no verbal subsidiary agreements. Any other agreements or agreements deviating from the provisions set out in this contract shall only be effective if they are agreed in writing. This also applies to the cancellation of this clause.

11.2. *(special arrangements between the parties)* / -does not apply-

11.3 Should one or more provisions of this contract be wholly or partially ineffective or unenforceable, the validity of the remaining provisions shall remain unaffected. The ineffective or unenforceable provision shall be replaced by the contracting parties with a valid provision which comes closest to the intended purpose of the ineffective clause.

Annex: General technical and organisational measures pursuant to Article 25 (1) and Article 32 of the GDPR

1. Access control

Measures must be taken to prevent unauthorised access – in the spatial meaning of the term.
Technical or organisational measures for access control, especially in regard to legitimizing authorised persons:

- Providing a central reception area
- Ensuring that outsiders are only permitted in any part of the company's buildings if members of staff are also present
- Logging of employees arriving and leaving the building
- Designating individuals who are authorised to enter the computer/server room
- Providing key control (locked doors; issuing of keys to authorised individuals only; storage and use of a master key)
- Ensuring that building security based on an alarm system
- Providing a manual locking system with security locks
- Logging of visitors
- Ensuring careful selection of cleaning staff

2. Entry control

Measures must be taken to prevent intrusion of unauthorised persons into data processing systems.
Technical (password/password protection) and organisational (user master record) measures regarding user identification and authentication:

- Identifying users by password to the data processing system
- Authenticating users by password
- Drawing up and enforcing rules for personal password allocation (a minimum of 8 characters, including special characters/numbers, allocation by the user him/herself, no issuing to third parties, arrangements in the event of absence (leave, illness, etc.))
- Ensuring the immediate blocking of permissions when employees cease to work for the company
- Carrying out regular checks on the validity of permissions
- Securing VDU workstations when staff are absent and when the system is running
- Isolating of internal networks to prevent external access (firewall and VPN)
- Assigning user profiles to IT systems
- Encrypting of smartphone content
- Using anti-virus software
- Using a software and hardware firewall

3. Admission Control

Measures must be taken to prevent unauthorised activity in data processing systems outside the scope of any permissions that have been granted. Demand-based design of the authorisation policy and access rights, and the monitoring and logging of these:

- Drawing up and implementing an authorisation scheme
- Reducing the number of administrators to what is actually required
- Logging accesses to applications, especially when entering, changing and deleting data
- Organising administration of rights by a system administrator
- Drawing up and enforcing rules for personal password allocation (a minimum of 8 characters, including special characters/numbers, allocation by the user him/herself, no issuing to third parties, arrangements in the event of absence (leave, illness, etc.))
- Encrypting data media
- Ensuring proper destruction of data media
- Logging of the destruction of data media

4. Transfer control

Measures must be taken for the secure transport, transfer and transmission or storage on data carrier (manual or electronic) and to carry out subsequent checks:

- Encrypting data transfer
- Using dedicated lines or VPN tunnels
- Documenting data recipients and time periods for the planned transfer or agreed deletion periods
- Requiring all employees to comply with the data protection requirements of the General Data Protection Regulation (REGULATION (EU) 2016/679)

5. Input control

Measures must be taken to ensure the traceability and documentation of data management and maintenance. Measures must be taken to ensure subsequent checking of whether data has been entered, modified or removed (deleted) and to record who carried out such action:

- Logging and traceability of data entry by users
- Granting of rights to enter, change and delete data based on an authorisation scheme

6. Order control

Measures must be taken to guarantee order data processing in accordance with the instructions. Measures (technical / organisational) for the division of responsibilities between the Customer and the Contractor:

- Selecting contractors according to aspects of due diligence
- Drawing up data processing contract involving contractors and customers
- Ensuring the destruction of data after the end of the contract
- Conducting ongoing reviews of the Contractor and the Contractor's activities

7. Availability and capacity

Data must be protected against any accidental destruction or loss.

Measures for data protection and back-up (physical/logical):

- Uninterruptible power supply (UPS) is guaranteed
- Data hosting by cloud providers
    - Emergency manuals with defined responsibilities
    - Regular, documented data back-up
    - Storage of back-ups in a location other than the system that is being backed up
    - Limited access to back-up software on dedicated back-up administrators
    - Carrying out a random functionality test of data back-ups
    - Secure deletion and overwriting procedures (BSI recommendations) of the storage media of data back-ups
    - Highly redundant network infrastructure
    - Early fire detection system and argon extinguishing system

Rapid recoverability (Article 32 (1) (c) of the GDPR)

- Conducting of regular data recovery tests
- Documented emergency plan
- Documented back-up & recovery system
- Data hosting by cloud providers
    - Regular, logged and documented checking of the recovery plan of the systems
    - Regular, logged and documented simulations of emergency situations
    - Testing the escalation paths in real-life operation
    - Storage of back-ups in a location other than the system that is being backed up

8. Separation control

Data collected for different purposes must also be processed separately. Measures for the separate processing (storage, modification, deletion, transmission) of data with different purposes:

- Arranging physically separate storage on separate systems or data media
- Drawing up and implementing an authorisation scheme
- Establishing database rights
- Ensuring logical client separation (in terms of software)
- Separating productive and test systems

9. Pseudonymisation (Article 32 (1) (a) of the GDPR)

Data is not pseudonymised.

10. Procedure for regular review, assessment and evaluation of the effectiveness of technical and organisational measures to ensure the safety of processing (Article 32 (1) (d) of the GDPR)

Data protection management and notification of data breaches (Article 33 of the GDPR)

- Regular review and continuous improvement of the data protection policy
- Regular review and continuous improvement of the processing directory
- Conducting regular employee training
- Conducting risk assessments
- Performing regular penetration tests
- Regular update of the software and hardware firewall
- Regular update of anti-virus software