Data Processing Agreement

between

FUMO Solutions’ customer

– Controller within the meaning of Article 24 of the GDPR,
hereinafter referred to as the “**Customer**” –

and

FUMO Solutions GmbH
Lerchenbergstraße 27
89160 Dornstadt
Germany

– Processor within the meaning of Article 28 of the GDPR,
hereinafter referred to as the “**Contractor**” –

Last revision: 29/1/2020

1. Subject matter and term

.1 The subject matter of this Data Processing Agreement (“DPA”) is the performance by the Contractor of its tasks in accordance with the agreement concluded between the Parties (“Services Agreement”) which was formed using the registration process for the relevant modules (including any future modules) or by placing a written order.

1.2 The term of this DPA shall correspond to the term of the Services Agreement which was formed using the registration process for the relevant modules (including any future modules) or by placing a written order.

2. Specification of the subject matter

2.1 The nature and purpose of the Contractor's tasks is set out in the Services Agreement.

2.2 The commissioned processing shall take place only in a member state of the European Union or another state which is a signatory to the Agreement on the European Economic Area. Any transfer to a Third Country is subject to the Customer’s prior written approval and may only take place if the special requirements set out in Article 44 et seq. of the GDPR are met.

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

- Personal master data
- Communication data (e.g. telephone, e-mail)
- Contract master data (contractual relationship, interest in products or contracts)
- Customer history
- Contract billing and payment data
- Planning and control data
- Information (from third parties such as credit agencies or from public directories)
- Data relating to employees' jobs as drivers such as categories of driving licences, driving times, vehicles driven and contracts

2.4 The categories of data subjects in the context of this DPA include:

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

3. Technical and organisational measures

3.1 The Contractor shall be obliged to document the implementation of the technical and organisational measures detailed prior to placing the order before the processing starts (particularly with regard to the specific implementation of this DPA) and to provide them to the Customer for review. If accepted by the Customer, the documented measures shall become the contractual basis for the commissioned processing. 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 and shall ensure that personal data is lawfully processed in accordance with Article 5 of the GDPR. Overall, the measure to be taken are data security measures in order to ensure a level of protection appropriate to the level of risk in terms of the confidentiality, integrity, availability and resilience of systems. The state of the art, implementation costs and the nature, scope and purposes of processing as well as the varying likelihood 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 adequate measures. These may not fall below the level of security of the specified measures. Significant changes shall be documented.

4. Rectification, restriction of processing and erasure of data

4.1 The Contractor may rectify, erase or restrict der processing the data processed on behalf of the Customer only on documented instructions from the Customer. If a data subject contacts the Contractor directly to have their data rectified or erased, the Contractor shall immediately forward this request to the Customer.

4.2 Insofar as this is within the scope of the Services Agreement, the erasure policy, the right to be forgotten, rectification, data portability and the right of access by the data subject are to be ensured by the Contractor itself in accordance with the Customer’s documented instructions.

5. Quality assurance and other obligations of the Contractor

In addition to complying with the provisions hereunder, the Contractor shall have the following obligations in accordance with Articles 28 to 33 of the GDPR, in particular:

— Designation in writing of a data protection officer who is able to carry out his/her tasks in accordance with Articles 38 and 39 of the GDPR. The Customer shall be notified of the data protection officer’s contact details, allowing the Customer to make direct contact with the data protection officer. The Customer shall be notified without undue delay of any replacement of the data protection officer.

— Maintaining confidentiality in accordance with Article 32(4) of the GDPR. Any persons authorised to access the Customer’s personal data in the context of the commissioned processing must first have been obliged to maintain confidentiality and have been informed about the relevant data protection requirements. The Contractor, and any person acting under the authority of the Contractor who has access to personal data in the context of the commissioned processing, may, in accordance with Article 29 of the GDPR, process such data only on instructions from the Customer unless they are required to process the data by Union or Member State law.

— Implementation of and compliance with all technical and organisational measures required for the commissioned processing in accordance with Articles 25 and 32 of the GDPR and the **Annex** hereto.

— On request by a supervisory authority, the Customer and the Contractor shall cooperate in carrying out their duties.

— Notification of the Customer without undue delay of any investigatory activities or measures by the supervisory authority with regard to the commissioned processing. This shall also apply if a competent authority carries out investigations into the Contractor as part of regulatory offence or criminal proceedings.

— In the event of the Customer being subject to investigations by the supervisory authority in regulatory offence or criminal proceedings, liability claims of a data subject or a third party or any other claim relating to the commissioned data processing carried out by the Contractor, the Contractor will use its best efforts to support the Customer.

— Using regular checks to ensure commissioned data processing compliance with regard to the performance of this DPA. This relates, in particular, to compliance with and any necessary adaptations of the provisions and measures for carrying out this DPA to ensure that the processing by the Contractor is lawful and the protection of the of the data subjects' rights is ensured.

— The ability to demonstrate the technical and organisational measures to the Customer. For this purpose, the Contractor may provide up-to-date certificates, reports or extracts from reports from independent bodies (e.g. accountants, auditors, data protection officers, IT security departments, data protection auditors, quality auditors) or appropriate certification by an IT security or data protection audit (e.g. in accordance with the „BSI Grundschutz" ["Basic Protection" guidelines published by the German Federal Office for Information Security]).

6. Subcontracting

6.1 Where any subcontractor (another processor within the meaning of Article 28 of the GDPR) is to be involved in the processing or use of the Customer's personal data, this shall be autorised if the following conditions are met:

— As a rule, the involvement of subcontractors is only permitted with the Customer's approval in writing (a fax or e-mail shall suffice). Without such consent, the Contractor may use subcontractors for the performance of this DPA, subject to compliance with statutory diligence and the obligation to ensure commissioned data processing compliance set out in section 5 provided that the Contractor has notified the Customer of this prior to the start of the processing in writing on an electronic medium and the Customer has not objected to the relocation of the data processing within one month of the receipt of the notification in writing on an electronic medium.

— The Contractor shall draw up the contractual provisions agreed with the subcontractor in such a way that they comply with the data protection provisions under the DPA 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 with respect to the subcontractor in accordance with this DPA. This includes the right of the Customer to obtain from the Contractor, on written request, information about the key content of the contract and the implementation of the data protection obligations under the agreement with the subcontractor, if necessary by review of the relevant contractual documents.

— The involvement of the subcontractor shall not be permitted unless all of the above requirements are met.

— The above requirements shall apply accordingly if the subcontractor itself wishes to enter into an agreement with a subcontractor.

— The Contractor herewith authorises the involvement of the following subcontractor: 1&1 Internet SE, Elgendorfer Str. 57, 56410 Montabaur (DE) (hosting the web platform)

6.2 For the purpose of the above provisions, services that the Contractor uses as ancillary services provided by third parties as assistance in the performance of the commissioned processing shall not be deemed to be subcontracting. These include, for example, telecommunication services, maintenance and user support, cleaners, auditors. Notwithstanding the Contractor shall be required to make agreements which are appropriate and conforming to the law and to take control measures to ensure the protection and security of the Customer's data where ancillary services are provided by third parties.

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 employed by the subcontractor in accordance with paragraph 6.2, the Contractor shall ensure that the processing of personal data is lawful.

7. Inspection rights of the Customer

7.1 The Customer has the right to carry out inspections after consultation with the Contractor or to have such inspections carried out by an inspector who is to be designated for a specific case. The Customer has the right to carry out spot inspections, which as a rule shall be notified to the Contractor in good time, to verify the Contractor's compliance with this DPA on-site. The Contractor undertakes to provide the Customer with the information required to comply with the Customer's obligations under Article 28 of the GDPR and to provide appropriate evidence.

7.2 In regard to the Customer's inspection obligations prior to the start of the data processing and during the term of this DPA, the Contractor shall ensure that the Customer can verify compliance with technical and organisational measures taken. Accordingly, on request the Contractor will inform the Customer of the implementation of the technical and organisational measures in accordance with Articles 25 and 32 of the GDPR and the **Annex**. The evidence of the implementation of measures which are not only relevant for the specific commissioned processing, 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 mechanism pursuant to Article 42 of the GDPR.

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 any statutory provision on the protection of the Customer's personal data or any provision hereunder.

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 an adequate level of protection by putting in place technical and organisational measures that take into account the context and purposes of the processing, as well as the predicted likelihood and severity of a possible infringement of rights by security vulnerabilities, and enable the immediate detection of relevant security breaches.

— undertaking to notify the Customer of any personal data beaches without undue delay.

— undertaking to assist the Customer with regard to the Customer’s obligation to communicate a personal data breach to the data subject and to provide the Customer with any relevant information without undue delay.

— Assisting the Customer with any data protection impact assessment.

— Assisting the Customer in the context of prior consultations with the supervisory authority.

9. The Customer’s right to give instructions

9.1 The processing of data takes place only within the scope of this DPA and in accordance with the Customer’s instructions (cf. Article 29 of the GDPR). Within the scope of the subject matter defined hereunder, the Customer reserves a comprehensive right to issue instructions regarding the nature, scope and means of the data processing, which the Customer may exercise by issuing specific instructions. Changes to the subject matter of the processing and procedural changes shall be jointly agreed and shall be documented. The Contractor may only give information to third parties or the data subject to the Customer’s prior written consent.

9.2 The Customer shall confirm any oral instructions in writing (a fax or e-mail will suffice) without undue delay. The Contractor shall not use the data for any other purposes and, in particular, is not authorise to disclose data to third parties. No copies or duplicates shall be made without the Customer’s knowledge. This does not include back-up copies – if these are necessary 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 shall processes the personal data, in accordance with clauses 9.1 and 9.2 only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

10. Erasure of data and return of data carriers

10.1 The Contractor is not authorised to make copies of the personal data. This shall not apply to back-up copies, where necessary to ensure that data processing is carried out in the proper manner, and data which is necessary to comply with statutory retention requirements.

10.2 After completion of the Contractor’s contractual tasks or earlier on request by the Customer – but no later than the termination of the Services Agreement – the Contractor shall deliver to the Customer all documentation, any results derived from the processing and usage of data, as well as existing data pertaining to the commissioned processing, or destroy them in accordance with data protection law. The same applies to test and scrap material. A report of such erasure shall be submitted on request.

10.2 The Contractor shall retain documentation serving as evidence of proper processing in compliance with this DPA beyond the termination of the commissioned processing in accordance with respective retention periods. The Contractor may deliver them to the Customer in discharge of its obligation on termination of this DPA.

11. Final provisions

11.1 This DPA is a supplement to the Services Agreement Services Agreement which was formed using the registration process for the relevant modules (including any future modules) or by placing a written order. There are no verbal subsidiary agreements. Any other agreements or agreements deviating from the provisions set out in this DPA shall only be effective if they are agreed in writing. This shall also apply to any waiver of the requirement of the written form

11.2 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.

In case of a written order sign here.

For the Contractor

Dornstadt, ___________

____

(FUMO Solutions)

For the Customer

____________________, _________

(Place) (Date)

____

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

1. Physical access control

Measures must be taken to prevent unauthorised physical access – in terms of entry to premises.

Technical or organisational measures for entry control, especially in regard to legitimising 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. Data access 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. Data usage 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:

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

6. Commissioned data processing compliance 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 due diligence
- Data processing agreementa with controllers and processors
- Ensuring the destruction of data after the termination of commissioned data processing
- Conducting ongoing reviews of the Contractor and the Contractor's activities

7. Availability and resilience

Data must be protected against any accidental destruction or loss.
Measures for backin-up data (physical/logical):

- Uninterruptible power supply (UPS) is ensured
- 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
  - Access to back-up software s limited to dedicated back-up administrators
  - Carrying out random functionality tests of data back-ups
  - Secure erasure and overwriting procedures (according to recommendations by the German Federal Office for Information Security) of the storage media of data back-ups
  - Highly redundant network infrastructure
  - Early fire detection system and argon extinguishing system

Ability to restore the availability and access to personal data in a timely manner 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, erasure, 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. Process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the 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