ANNEX

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with [choose relevant option: OPTION 1: Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data] / [OPTION 2: Article 29(3) and (4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data].

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 - Optional

Docking clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause7

Obligations of the Parties

7.1. Instructions

(a) The processor shall process personal data 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 this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a) OPTION 1: PRIOR SPECIFIC AUTHORISATION: The processor shall not subcontract any of its processing operations performed on behalf of the controller in accordance with these Clauses to a sub-processor, without the controller's prior specific written authorisation. The processor shall submit the request for specific authorisation at least [SPECIFY TIME PERIOD] prior to the engagement of the sub-processor in question, together with the information necessary to enable the controller to decide on the authorisation. The list of sub-processors authorised by the controller can be found in Annex IV. The Parties shall keep Annex IV up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION: The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least [SPECIFY TIME PERIOD] in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in [OPTION 1] Article 32 Regulation (EU) 2016/679/ [OPTION 2] Articles 33, 36 to 38 Regulation (EU) 2018/1725.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to [OPTION 1] Article 33(3) Regulation (EU) 2016/679/ [OPTION 2] Article 34(3) Regulation (EU) 2018/1725, shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to [OPTION 1] Article 34 Regulation (EU) 2016/679 / [OPTION 2] Article 35 Regulation (EU) 2018/1725, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller’s obligations under [OPTION 1] Articles 33 and 34 of Regulation (EU) 2016/679 / [OPTION 2] Articles 34 and 35 of Regulation (EU) 2018/1725.

SECTION III – FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I LIST OF PARTIES

1. Controller(s):

The company name and address of the responsible party are indicated in the offer of SEMA GmbH Computer Software und Hardware-Vertrieb.

A separate signature of these standard contract clauses by the responsible party is not required. These standard contract clauses are an integral part of the subscription contract. By countersigning the offer of SEMA GmbH Computer Software und Hardware-Vertrieb to conclude the subscription contract by the responsible party these standard contract clauses are also legally binding.

2. Processor(s):

Name: SEMA GmbH Computer Software und Hardware-Vertrieb
Address: Salzstraße 25, 87499 Wildpoldsried

Contact person's name, position and contact details:

Claudia Kirchgessner
Head of Backoffice
Signature: ____________________________

Silvia Emilius
Backoffice
Signature: ____________________________

Data protection officer: Joachim Hanke

ANNEX II TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

Technical and organisational measures

1. Pseudonymisation

There is direct processing of personal data mentioned in the order. The possible visibility or access to personal data exists. Pseudonymisation or anonymisation does not take place.

2. Encryption

All mobile data carriers are encrypted according to the state of the art. The internal IT guidelines regulate the handling of data and their storage.

3. Guarantee of confidentiality

Access control:	The type of building is an office building used only by the companies SEMA GmbH and WGsystem GmbH. The entrance doors are secured by a security lock with an electric motor. These locks can only be opened by means of a chip card. To the outside, the entrance doors are equipped with a rigid door knob instead of a handle and are locked by the motor lock outside business hours. Staff records are locked in filing cabinets outside business hours. The server room is also secured by a security lock with an electric motor, which can only be opened by a chip card. This room is locked around the clock. Chip cards are issued exclusively to authorised persons and are immediately withdrawn if the authorisation expires. The authorisation to enter is recorded and documented by appropriate measures. If an access device is lost or if a former authorised person does not voluntarily return an access device, the access device is blocked individually. The window type of the building and the office and business premises is triple insulated glazing. The windows are closed in all locations outside business hours. Strangers are only permitted to stay in the entire company building in the presence of employees. Auxiliary persons are always carefully selected. There is a chip card with access authorisation to all three external doors at the Wildpoldsried Volunteer Fire Brigade in a safe provided for this purpose.
Access and Access control	A password system is in place for access to the data processing systems. A password policy has been established. Each authorised person receives an individual user ID and a personal password that must be kept secret and may not be passed on to third parties. There is a regulation in case of absence. Authorisations are checked regularly. The password is locked if the authorisation expires. The password consists of at least 14 characters (randomly selected upper case letters, lower case letters, special characters and numbers). After three unsuccessful attempts, the user ID is blocked. Internal networks are protected against external access by a complete physical separation of internal and external networks according to the state of the art. A firewall with at least daily software updates is installed. External connections are secured via https and certificates. The access of users is logged when they log in and log out. Organisational requirements such as organisational charts, job descriptions and task descriptions are in place. These are regularly updated and implemented in role definitions. Role allocation is reviewed regularly. An authorisation concept is in place. Within the access authorisation concept, graduated access authorisations are set up that only allow the entry, reading, copying, modification or removal of client data during processing, use and after storage to the extent required for the respective task and otherwise prevent it. The access authorisation concept includes the management of access rights by system administrators. Test operation is separated from production operation. Internet and e-mail use is controlled and organised, and private Internet and e-mail use in the company is also regulated. Areas where data media are stored are specially secured. Data carriers and misprints that are no longer needed are disposed of in accordance with data protection regulations.
Separation control	The data is stored for more than one responsible body, the storage takes place in a multi-client capable database. The purposes for which the respective data are to be processed and used are documented. Access rights are clearly defined. A concept for data collection and processing is in place. The production networks are physically separated from the test network by appropriate measures. The security level of the test systems is as high as that of the production systems. It is ensured that production data is only used as test data after consultation with the client.

4. Guarantee of availability	
Availability control	The contractor shall ensure sufficient software protection against the violation of system integrity by memory-resident scanners against viruses, Trojans, worms and other malware. The execution of non-workstation software shall be prevented by contractual prohibitions of users, spam filters, licence monitoring and at least daily updating of the operating system, the existing operating and security software. Sufficient hardware protection is ensured by an uninterruptible power supply and compliance with the relevant fire protection regulations. A data security concept is in place. This concept provides for backup copies to be made according to the generation principle at appropriate intervals. The data stock is backed up incrementally at least once a day and completely encrypted on external storage media once a week. A weekly full backup is stored in the data centre of IDKom Networks. An emergency manual/emergency concept is available.
Control of data carriers	When readable data carriers are handed over, it is ensured that there is no residual data on them, for example from other processing operations.

5. Guarantee of integrity	
Transfer control	The data transmission takes place via a fibre optic connection of Telekom via synchronous VDSL, the purpose of the transmission is order processing. The participants are identified and authenticated. Authentication takes place via a user ID and password. Mobile data carriers with client data, mobile end devices with client data and USB ports may only be used by employees specifically authorised to transfer and secure data for contractual and security purposes only. The password consists of at least 14 characters (randomly selected upper case letters, lower case letters, special characters and numbers). Generic terms or proper names may not be used. Documentation of data recipients is provided. Data media are destroyed by Mr. Joachim Hanke and the Dorr company. Until their destruction, the data media are stored in the locked warehouse of the Technology Department. There is an agreement on order processing with an external service provider.
Input control	Unauthorised entries, changes and deletions are prevented by a password system. The entry, modification or deletion of personal data is recorded in an audit-proof manner. The input authorisations are maintained in an audit-proof manner and issued in writing. The input authorisations are regulated on created log data. As a central measure, the system logs are regularly evaluated in the input control. The system logs are evaluated anonymously and the users concerned are only identified if there is a specific reason to do so. There is a deletion regulation for log data. All staff are bound to confidentiality. The following applications have a second access control: ADITO, Outlook, SAGE, BBS Reisekosten, HR Works, all banking software, Docuguide, WGsystem. However, the following applications do not have a second access control: SEMA Holzbausoftware, all Office programs except Outlook.

6. Recovery of data

We have our own comprehensive backup concept and an emergency manual. Backup software from renowned manufacturers is used.

7. Ongoing assessment and evaluation

A data protection guideline has been implemented. A data protection officer has been appointed and is regularly trained in data protection. Employees are regularly instructed in data protection matters. A data breach notification process has been implemented. The technical and organisational measures are audited annually by the Data Protection Officer and the Head of IT. Within the scope of the audit, the measures are checked regarding the state of the art as well as the necessary technical and legal requirements and adjusted if necessary. The result of the audit is documented accordingly.