End User Agreement for RSP Connect

IMPORTANT: READ THE FOLLOWING CAREFULLY BEFORE USING THE TELEMATICS SERVICES: This End User Agreement ("EUA") is a legal agreement between you, the End Customer or End User (both defined below), and RSP GmbH ("OEM") for your licensed use of the Telematics Service, and the OEM's Licensor (defined below) is a third party beneficiary under this EUA. By accepting this EUA or activating, accessing or otherwise using the Telematics Service, you agree to be bound by the terms of this EUA as a condition of your license and use of the Telematics Service. You will be asked to review the terms of this EUA and either accept or not accept them. If you do not agree to the terms of this EUA, you are prohibited from using, activating, accessing or otherwise using the Telematics Service.

1. Definitions.

"Subscription" means the end user subscription to the Telematics Service provided by the OEM.

"Subscription Term" means the term of the End User Subscriptions specified in the Price List.

"Activation Date" means the date on which the End Customer or any of its End Users first activates the Telematics Service or the other commencement date of the Telematics Service as determined between the End Customer and the OEM.

"Malicious Code" means a code, files, scripts or programs designed to cause harm, including, for example, viruses, worms, malware and Trojans.

"Data Platform" means the cloud-based data platform together with Web Portal, Realtime Client, REST API and other IT systems on and through which the Software operates the Telematics Service, stores the Machine Data and provides licensed access to End Customers and their End Users under the Subscription.

"Derivative" means all derivatives, modifications, error corrections, patches, bug fixes, metadata, configuration and calibration settings, software updates, upgrades, en- hancements, extensions and subsequent releases of the Software, regardless of the creator.

"End Customer" means the business entity entitled by subscription to use the Telematics Service obtained by the OEM from its Licensor.

"End User" means the employees and temporary staff of the End Customer authorised by it to use the Telematics Service on its behalf in accordance with the provisions of this EUA.

"Firmware" means the software and/or application programming interface embedded in the communication unit (CU) connected to the machine, including adaptations or other derivatives thereof (whoever is the creator), in order for the CU to be compatible with the communication protocol of the machine and to communicate.

"Licensor Intellectual Property" means the Firmware, the Software, the Data Platform, the Web Portal, the Manuals and the Telematics Service.

"Manuals" means the user and installation instructions provided in electronic or printed form in connection with the Telematics Service.

"**Communication Units"** or **"CUs"** means the onboard hardware devices factory-installed by the OEM in the Vehicles sold to the End Customer that transmit End Customer Machine Data to and from the Data Platform and provide subscribed and licensed access to the End Customer and its End Users via the Web Portal.

"Licensor" means the Software Publisher.

"Machine" means a vehicle, or other asset containing a Communication Unit, used in the End Customer's business for which Machine Data is transmitted via the Telematics Service.

"Machine Data" or **"Telemetry Data"** means: (a) the raw machine-readable data collected by the Communication Units and transmitted to the Data Platform, and (b) the useful data obtained therefrom by the Telematics Service in the form of individual or aggregate data about an End Customer's Machines, such as status, geographic location, hours of operation and other vehicle-related Machine data transmitted between the Data Platform and the CUs.

"Mobile Communication Service" means any communication standard used by the Communication Units, e.g.

LTE, 5G, or any other communication for the transmission of Machine Data to and from the CUs and the Data Plat- form.

"OEM" means the Original Equipment Manufacturer who, as the Service Provider, provides the Telematics Ser- vice to the End Customer.

"Telematics Service" or **"RSP Connect"** means the online service provided by the Software on the Data Platform and accessed by End Customers and their End Users un- der the Subscription and this Licence via the Web Portal that maps and controls Machine Data transmitted to and from the CUs installed in the Machines.

"Web Portal" means the website configured in the name and brand of the OEM through which End Customers and their End Users may obtain online access to use the Telematics Service.

2. granting of a limited licence for the telematics service.

(1) On the Activation Date and during the Subscription Term, the OEM hereby grants to the End User and its End Users (on behalf of the Licensor) a limited, terminable, personal, non-exclusive and non-transferable licence:

(a) Licence to use the firmware,
(b) Licence to use the Software,
(c) right to access and use the Telematics Service via the Web Portal (to the extent of the Service Level) for the End Customer's internal business purpose of enabling its End Users to monitor and control Machines; and
(d) licence to use the resulting machine data generated by the Telematics Service and sorted on the Data Platform, expressly excluding:
(i) any use by users other than the subscribed end-user and its end-users;
(ii) any use with CUs or other devices not licensed by the Licensor; and
(iii) any use for machinery other than machinery of an end user.

(2) The Customer Application integrates functions and contents of *OpenStreetMap of* the service provider O-penstreetmap Foundation. The respective current versions of the terms and conditions of the service provider shall apply to the use: (i) Terms of Use for *OpenStreetMap* at https://wiki.osm- foundation.org/wiki/Terms_of_Use; and (ii) OSM Privacy Policy at https://wiki.osmfoundation.org/wiki/Privacy_Policy.

3. licence restrictions.

Neither the end customer nor its licensed end users may: (a) use, make available to or permit the use by any third party of any aspect of the Telematics Service or the Li- censor's other intellectual property,

(b) transfer, sell, rent, loan, disclose, use for timesharing or outsourcing purposes the Licensor's Intellectual Property or any other aspect of the Telematics Service,
(c) use the Telematics Service or the Licensor's other intellectual property to store or transmit infringing, defamatory or otherwise unlawful or tortious material or to store or transmit material which infringes the privacy rights of third parties,
(d) use the Telematics Service or the Licensor's other intellectual property to store or transmit malware,

(e) attempt to gain unauthorised access to any aspect of the Telematics Service or other intellectual property of the Licensor,
(f) copy the Telematics Service, the Licensor's other intellectual property or any part, feature, function or user interface thereof,

(g) reverse engineer, decompile, translate, disassemble or attempt to discover the source code or underlying ideas or algorithms of Licensor's Intellectual Property or otherwise use Licensor's Intellectual Property other than as permitted herein or attempt to obscure or remove any copyright, trademark or other notices appearing on any Licensor's Intellectual Property.

This Section 3 shall survive the termination of this EEA.

4. intellectual property of the licensor.

The Limited Licence and the rights granted to you under Section 2 do not confer any right or ownership in the Licensor's Intellectual Property and shall not be construed as a sale of any rights in the foregoing Content. Subject to the Limited Licence and the rights granted to you under Section 2, the Licensor retains all right, title and interest in and to all Intellectual Property, including: (a) any derivative works, improvements, enhancements, corrections or customizations to the foregoing Content, whether created or developed by you and/or the Licensor , and (b) any suggestions, recommendations or other feedback provided by you. Nothing in this EUA grants you any right to the source code of the Software. This

Section 4 shall survive the termination of this EUA.

5. data protection agreement in accordance with Art. 26 EU General Data Protection Regulation (GDPR) between the end customer and the OEM on the processing of personal machine data.

(1) The Telematics Service may be based on the processing of personal machine data, for example when end customers use it to manage machines operated by per- sons identifiable above. In this Agreement, the terms "personal data" and "controller" shall have the meaning assigned to them in the GDPR.

(2) The OEM shall provide the End Customer with certain vehicle and fleet management functions in the Web Portal for the duration of the subscription, including the geolocation of vehicles assigned to him, evaluations of certain machine data, the deactivation/activation of certain machine functions and end user management, in each case in accordance with the configuration by the End Customer. The data processing required for the provision of these functions is carried out by the OEM as the end customer's processor in accordance with Art. 28 GDPR (Annex 1).

(3) The OEM shall use the machine data as the responsible party for its own purposes, for research, development and analysis purposes within the scope of the legitimate interest to improve its products and services, as well as to develop new machine functions, where possible pseudonymised or anonymised. In addition, by processing the machine data, the OEM fulfils its product monitoring and road safety obligations. Location data is processed for statistical evaluations of regions of use, for planning and expanding the service partner network, but also to be able to support the end customer in any investigations in the event of theft or loss during transfers. The OEM and the End Customer agree that, from the start of the subscription, both are deemed to be joint controllers within the meaning of Article 26 of the GDPR.

(4) In addition, the end customer and the OEM process the machine data as jointly responsible parties for the duration of the subscription in order to be able to derive machine-specific service intervals which, for example, trigger invitations to service inspections by authorised specialist workshops (individual customer service) or make claims for the rectification of defects objectively verifiable.

(5) By accepting this EUA, expressly or impliedly by activating, accessing or otherwise using the Telematics Service, you as the End Customer acknowledge and agree that, insofar as the persons affected by the Telematics Service are located in the European Economic Area, the following provisions are also agreed.

(6) This Agreement governs the rights and obligations of the End User and OEM (collectively the "Parties") in the joint processing of End User Personal Machine Data for the purposes set forth in Section 5 (4). This Agreement shall apply from the date of adoption of this EUA and shall apply to all activities in which employees of the Parties, or their agents, process personal machine data for the purposes set out in Section 5 (4).

(7) As the provider of the Telematics Service, the OEM shall fulfil all obligations pursuant to Art. 25, Art. 24 Para. 1, in conjunction with Art. 32 to 34 GDPR and Art. 28 GDPR. Art. 32 to 34 of the GDPR and Art. 28 of the GDPR and establish an appropriate level of security, in particular in connection with Art. 5 Para. 1, Para. 2 of the GDPR, insofar as these are not the responsibility of the end customer. Overall, the measures to be taken are data security measures and to ensure a level of protection appropriate to the risk with regard to confidentiality, integrity, availability and the resilience of the systems. The state of the art, the implementation costs and the nature, scope and purposes of the processing as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 (1) of the GDPR must be taken into account.

(8) The OEM is free to use processors or sub-processors at its own discretion. The OEM is responsible for verifying the suitability and compliance with the requirements of Art. 28 GDPR. The OEM shall inform the end customer in good time of any relocation of data processing to third countries.

(9) The legal basis for the processing of the machine data for the purposes named in section 5 (4) is the legitimate interest of the end customer and OEM in data-driven improvements in telematics and customer service as well as the most objective possible verifiability of claims for rectification of defects.

(10) The Parties agree to take all necessary technical and organisational measures to ensure that the rights of the data subjects, in particular in accordance with Articles 12 to 22 of the GDPR, can be or are guaranteed at all times within the statutory time limits.

(11) The parties undertake to provide free of charge to the data subject the information required under Articles 13, 14 and 26(2) of the GDPR in a precise, transparent, intelligible and easily accessible form and in plain and simple language. The Parties agree that the information on the processing of personal data shall be provided.

The Parties agree that the End Customer shall provide the necessary information in accordance with the first sentence.

(12) Data subjects may assert the rights to which they are entitled under Article 7 (3) and Articles 15 to 22 of the GDPR against all contracting parties. The Parties agree that requests pursuant to sentence 1 shall be forwarded to the end customer without delay and processed there. If necessary, the Parties shall provide each other with the necessary information as well as the contact persons from their respective areas of responsi- bility. A change of the respective contact person shall be notified to the other party without delay.

(13) If personal data is to be deleted, the parties shall inform each other in advance. Either party may object to the deletion, provided that a legal obligation to retain data or another legal regulation precludes this.

(14) All parties are subject to the notification and communication obligations resulting from Articles 33 and 34 of the GDPR vis-à-vis their respective competent supervisory authority and the persons affected by a personal data breach for their respective area of responsibility. The Parties shall inform each other without undue delay of the notification of personal data breaches to their respective competent supervisory authority or other requests by the supervisory authority regarding the jointly processed personal machine data.

(15) End User agrees to use reasonable efforts in a timely manner to cooperate with OEM in responding to any such regulatory enquiries. The End User is not authorised to act or respond on behalf of the OEM.

(16) The end customer undertakes to arrange for the deletion of his account in the Web Portal and the data stored therein before selling his vehicle equipped with a CU. To this end, he will send the OEM a corresponding deletion request in good time. The OEM will then delete or anonymise the end customer's personal machine data assigned to the end customer.

7. technichal support.

The Licensor does not provide direct technical support for the Telematics Service, the Software, the Web Portal, the CUs or the Mobile Service ("**Support Items"**) to the End Customer or its End Users. The OEM is solely responsible for providing technical support to End Customers and/or End Users on the terms agreed between the OEM and the End Customer.

8. limitation of the warranty.

LICENSOR MAKES NO REPRESENTATIONS OR WARRANTIES TO END USER OR ITS END USERS WITH RESPECT TO THE TELEMATICS SERVICE OR ANY OTHER SUPPORT ITEMS. ALL REPRESENTATIONS AND WARRANTIES WITH RESPECT TO THE SUPPORT ITEMS, WHETHER WRITTEN OR ORAL, ARE HEREBY EXPRESSLY DISCLAIMED, AS ARE ANY IMPLIED REPRESENTATIONS AND WARRANTIES OF - MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. The OEM is solely responsible for making warranties (if any) to End Users and/or End Users for the Sup- port Items (if any) on the terms agreed between the OEM and the End User. This Section 8 shall survive termination of this EUA.

9. limitation of liability.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL LICENSOR OR ITS AFFILIATES BE LIABLE FOR ANY INCIDENTAL, DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE OR OTHER DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE TELEMATIK SERVICE OR IN CONNECTION WITH THE COLLECTION OF THE MACHINE DATA, WHETHER BASED IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR OTHERWISE. THIS LIMITATION OF LIABILITY APPLIES EVEN IF LICENSOR OR ITS AF- FILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR IF A REMEDY FAILS OF ITS ESSENTIAL PURPOSE. This Section 9 shall survive the termination of this EUA.

10. Termination.

This EUA may be terminated at any time by: (a) termination of the Subscription, (b) termination of the Telematics Master Agreement between OEM and Licensor, (c) notice from Licensor to End User in the event that End User or its End Users breach any term of this EUA. Upon termina- tion of this EUA for any reason: (a) the licence granted in Section 2 and any other licences or rights granted else- where in this EUA shall automatically and simultaneously terminate; and (b) the End Customer and its End Users shall immediately cease using the Telematics Service and the Licensor.

11. Applicable Law. Jurisdiction.

This EUA shall be governed by the laws of the Federal Re- public of Germany, without regard to its conflict of law provisions and excluding the United Nations Convention on Contracts for the International Sale of Goods (CISG). The OEM shall choose the place of jurisdiction (optionally English language).

Annex 1

Data protection agreement pursuant to Art. 28 GDPR
on the provision of IT services

between

End customer

- Person responsible within the meaning of the GDPR, hereinafter referred to as "Principal" -

and

RSP GmbH

- Processor within the meaning of the GDPR, hereinafter referred to as "Contractor" -

Preamble

According to the will of the parties and in particular the Principal, this commissioned processing contract ("Contract") contains the commissioned processing order and regulates the rights and obligations of the parties in connection with the data processing pursuant to Art. 28 GDPR. It applies to all activities in which employees of the Contractor or recipients comissioned by the Contractor have access to personal data of the Client.

§ 1 Subject matter, nature and purpose of the processing

A. Type of Processing

The Contractor shall make the Telematics Service available to the Client (SaaS) and provide support in this respect.
(1) Provision, care and maintenance RSP Connect
(2) Support RSP Connect

B. The subject of the contract is the provision of the following services by the Contractor in relation to the following categories of personal data and data subjects:

No.	Subject matter and purpose of the processing	affected persons	categories of personal data
1,2	Collecting, recording, organising, arranging, storing, reading, querying, provi- ding, restricting, deleting or destroying personal data in the context	Machine operator and end user of the client	• Company data: e.g. company name, location, contact details for notification, organisational unit

	of provision, maintenance, care and support telematics service		• Vehicle or machine information: e.g. make, model or type, registration number, oil pressure, fuel level, battery level, operating hours, max. speed, diagnostic messages, threshold violations of the subscribed safety level, maintenance requirements, next maintenance • GPS-based working time data: e.g. parking, transport, working, standing times and, if applicable, mapped route or location data per vehicle or machine • User profile data: e.g. user name, first name, last name and e-mail address and assigned role as well as password hash, login times and source IP address, selected time zone, language • CU data: e.g. serial number, eSIM number, assigned machine, signal strength and status data of the telemetry unit, configuration and/or modes

§ 2 Duration of the contract:

(1) This Agreement shall commence on the Activation Date and shall terminate upon the termination of the Subscription or the full performance by the Contractor of all Services required to be performed under the EUA.

(2) The right to extraordinary termination remains unaffected by this.

§ 3 Binding of the Contractor to Instructions

(1) The Contractor shall process the Client's personal data exclusively within the scope of the agreed provision of services and only on the basis of documented instructions, including with regard to the transfer of personal data to a third country or an international organisation, unless it is required to do so by the law of the Union or the Member States to which the Contractor is subject. In such a case, the contractor shall notify the controller of those legal requirements prior to the processing, unless the law concerned prohibits such notification on grounds of important public interest.

(2) Instructions deviating from the subject matter of the contract shall be issued by the Client or its authorised representative in writing by letter, fax or e-mail. The contractor shall confirm verbal instructions without delay (at least in text form).

(3) The Contractor shall not be permitted to correct, delete or restrict the processing unless it has received a corresponding written instruction from the Client. The Contractor shall not respond to any requests for information from data subjects regarding the processing operations covered by the contract, but shall forward any request for information to the Client without delay.

§ 4 Quality assurance and other obligations of the contractor

In addition to complying with the provisions of this contract, the Contractor shall observe statutory obligations pursuant to Articles 28 to 33 of the GDPR; in this respect, the Contractor shall in particular ensure compliance with the following requirements:

i. Written appointment of a data protection officer who performs his or her duties in accordance with Articles 38 and 39 of the GDPR. The current contact details of the data protection officer are easily accessible on the Contractor's website.

ii. Confidentiality pursuant to Art. 28 (3) sentence 2 lit. b, 29, 32 (4) GDPR must be ensured. When carrying out the work, the contractor shall only use employees who are bound to confidentiality and who have been fami- liarised with the data protection provisions relevant to them beforehand. The Contractor and any person sub- ordinate to the Contractor who has access to personal data may process this data exclusively in accordance with the Client's instructions, including the powers granted in this contract, unless they are legally obliged to process it.

iii. The implementation of and compliance with all technical and organisational measures required for this contract pursuant to Art. 28 (3) sentence 2 lit. c, 32 GDPR [details in the annex "Technical and organisational measures of the contractor (TOM)"].

iv. Keep a register of all categories of processing activities carried out on behalf of a controller in accordance with Article 30(2) where required by law.

v. The contracting authority and the contractor shall cooperate with the supervisory authority in the performance of its duties upon request.

vi. The immediate information of the client about control actions and measures of the supervisory authority, in- sofar as they relate to this order. This also applies insofar as a competent authority is investigating the Contrac- tor in the context of administrative offence or criminal proceedings with regard to the processing of personal data during the commissioned processing.

vii. Insofar as the Client, for its part, is exposed to an inspection by the supervisory authority, administrative offence or criminal proceedings, the liability claim of a data subject or a third party or any other claim in connection with the commissioned processing at the Contractor, the Contractor shall support it to the best of its ability.

viii. The contractor shall regularly monitor the internal processes as well as the technical and organisational measures to ensure that the processing in its area of responsibility is carried out in accordance with the requirements of the applicable data protection law and that the protection of the rights of the data subject is guaranteed.

ix. Verifiability of the technical and organisational measures taken vis-à-vis the Client within the scope of its supervisory powers pursuant to § 6 of this Agreement.

§ 5 Liability

(1) The client and the contractor shall be jointly liable vis-à-vis the respective data subject for any damage caused by processing that does not comply with the GDPR.

(2) The contractor shall be liable exclusively for damage resulting from processing carried out by him in which

i. the processor has not complied with the obligations resulting from the GDPR and specifically imposed on processors, or

ii. he acted in disregard of the lawfully given instructions of the principal, or

iii. he has acted contrary to the lawfully given instructions of the principal.

(3) Insofar as the Client is obliged to pay damages to the party concerned, it reserves the right of recourse against the Contractor.

(4) However, in the internal relationship between the principal and the contractor, the contractor shall only be liable for the damage caused by processing if it

i. has not complied with its obligations specifically imposed by the GDPR, or

ii. acted in disregard of or against the lawfully issued instructions of the principal.

(5) Further liability claims according to the general laws remain unaffected.

§ 6 Control rights of the principal

(1) The Client shall have the right to check the Contractor's compliance with the statutory provisions on data protection and/or compliance with the contractual provisions agreed between the parties and/or compliance with the Client's instructions to the extent necessary or to have the checks carried out by auditors to be named in the individual case.

(2) The contractor is obliged to tolerate these inspections. The Contractor shall provide information relating to the specific individual case without delay in response to enquiries from the Client and, in the event of inspections, shall provide evidence of compliance with this contract by means of suitable proof if requested to do so.

(3) The Contractor shall be obliged to provide the Client with information insofar as this is necessary to carry out the inspection within the meaning of paragraph 1.

(4) The Client may carry out the inspection within the meaning of paragraph 1 at the Contractor's or subcontractor's business premises at which the individual commissioned processing is carried out after prior notification with a reasonable period of notice during the respective normal business hours. The Client shall ensure that the inspections are only carried out to the extent necessary.

§ 7 Information duties

The Contractor shall assist the Client in complying with the personal data security obligations, data breach notification obligations, data protection impact assessments and prior consultations referred to in Articles 32 to 36 of the GDPR. This includes, among others

(1) ensuring an adequate level of protection through 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 potential security breach and allow for the immediate detection of relevant breach events;

(2) the obligation to notify the Principal without undue delay in the event of the loss or unlawful transmission or obtaining of knowledge of personal data of the Principal or other breaches of personal data;

(3) the obligation to assist the principal within the scope of his duty to inform the data subject and to provide him with all relevant information in this context;

(4) the support of the client for its data protection impact assessment;

(5) the support of the principal in the context of prior consultations with the supervisory authority.

§ 8 Subcontracting relationships

(1) Subcontracting relationships within the meaning of this provision shall be understood to be those services which directly relate to the provision of the main service. This does not include ancillary services which the contractor uses, for example, as telecommunications services, postal/transport services, maintenance and user service or the disposal of data carriers as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. However, the contractor is obliged to take appropriate and legally compliant contractual agreements as well as control measures to ensure data protection and data security of the client's data also in the case of outsourced ancillary services.

(2) The Contractor may engage subcontractors (further contractors) without the prior separate approval of the Client.

(3) Outsourcing to subcontractors or the change of existing subcontractors is permissible insofar as:

i. the contractor gives the principal reasonable advance notice in writing or text form of such outsourcing to subcontractors; and

ii. the Client does not object to the planned outsourcing in writing or in text form to the Contractor by the time the data is handed over, and

iii. a contractual agreement in accordance with Article 28 (2-4) of the GDPR is used as a basis.

(4) The objection to the intended change shall be raised with the Contractor within 4 weeks after receipt of the information about the change. In the event of an objection, the Contractor may, at its own discretion, perform the service without the intended change or - if the Contractor cannot reasonably be expected to perform the service without the intended change - terminate the service affected by the change vis-à-vis the Client within 4 weeks of receipt of the objection.

(5) The Client consents to the commissioning of the following subcontractors subject to the condition of a contractual agreement in accordance with Article 28 (2-4) of the GDPR:

No.	Name and address of other Contractors	Description of the partial services	Ort Place of performance
1,2	Proemion GmbH Donaustrasse 14 36043 Fulda	Software manufacturer Telematics Service as SaaS	EU
2	Subcontractor of Proemion GmbH: Atlassian.com Singel 236 1016 AB Amsterdam Niederlande	incident response	EU If applicable, also worldwide (standard contractual clauses)
2	Unterauftragsverarbeiter der Proemion GmbH: Salesforce Germany GmbH Erika-Mann-Str. 31 80636 München	CRM (support tickets)	EU If applicable, also worldwide (standard contractual clauses)

(6) The transfer of personal data of the Principal to the subcontractor and its first activity shall only be permitted once all requirements for subcontracting have been met.

(7) The Client shall be entitled to inspect the Contractor's contracts on commissioned processing and to demand that the Contractor send a copy of these contracts.

(8) The Contractor shall in particular be obliged to ensure by contractual provisions that the control powers of the Client and of supervisory authorities also apply vis-à-vis the subcontractor and that corresponding control rights of the Client and supervisory authorities are agreed and that on-site inspections in this respect are to be tolerated.

(9) A transfer to a third country may only take place if the special requirements of Art. 44 et seq. GDPR are fulfilled. The appropriate level of protection is established by standard contractual clauses and requires the prior consent of the client. The same applies if service providers as defined in paragraph 1 sentence 2 are to be used.

§ 9 Determination of technical and organisational measures

(1) The contractor shall ensure the implementation of the security measures required within the scope of the proper performance of the subject matter of the contract. It shall take appropriate technical and organisational measures for the adequate protection of personal data that meet the requirements of the General Data Protection Regulation, in particular Art. 32 GDPR. For this purpose, the contractor shall:

i. ensure the confidentiality, integrity, availability and resilience of the systems and services related to the processing on an ongoing basis,

ii. ensure the ability to rapidly restore the availability of and access to personal data in the event of a physical or technical incident; and

iii. take the measures illustrated in the Annex to this Agreement.

(2) The Contractor shall maintain a procedure to regulary review, assess and evaluate the effectiveness of the technical and organisational measures to ensure the security of the processing.

(3) The required technical and organisational measures are subject to technical progress and further development. In this respect, the contractor is permitted to implement alternative adequate measures. In doing so, the security level of the specified measures must not be undercut. Significant changes shall be documented and communicated to the Client.

(4) The Client is aware of the technical and organisational measures taken by the Contractor. The Client shall be responsible for ensuring that these provide an adequate level of protection for the risks of the data to be processed.

(5) The contractor shall organise the internal organisation in his area of responsibility in such a way that it meets the special requirements of data protection.

(6) He shall take the necessary technical and organisational measures to ensure a level of protection appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the varying likelihood and severity of the risk to the legal interests of the data subjects.

(7) The Contractor shall truthfully state all technical and organisational measures taken for the processing operations referred to in § 1 in the annex "Technical and organisational measures of the Contractor" to this contract. The Contractor shall ensure the verifiability of the technical and organisational measures taken vis-à-vis the Client within the scope of its supervisory powers.

§ 10 Ancillary obligations

(1) The contractor assures the client of the immediate proper destruction of data material that is not required (sample printouts, surplus lists, etc.).

(2) Copies and duplicates shall not be made without the knowledge of the client. This does not apply to security copies, insofar as they are necessary to ensure proper data processing, or to data that must be processed in order to comply with legal requirements.

(3) The Contractor shall name a contact person for the Client prior to the conclusion of the contract.

§ 11 Obligation beyond the end of the contract

(1) After completion of the contractually agreed work or earlier upon request by the Client - at the latest upon termination of the main contract - the Contractor shall hand over to the Client all documents that have come into its possession, processing and utilisation results produced as well as data files that are related to the contractual relationship or, after prior consent, destroy them in accordance with data protection law, unless there is a legal obligation to store the personal data.

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

(3) The contracting parties are obliged to maintain secrecy about the data that have become known in connection with the order, even after the end of the contractual relationship, and not to exploit them without written consent.

§ 12 Miscellaneous, General

(1) Amendments and supplements to this contract and all its components, including any assurances given by the Contractor, require a written agreement and express reference to the fact that it is an amendment or supplement to these terms and conditions. This also applies to the waiver of the formal requirement.

(2) Should individual provisions of this contract prove to be invalid or unenforceable in whole or in part or become invalid or unenforceable as a result of changes in legislation after conclusion of the contract, the remaining provisions of the contract and the validity of the contract as a whole shall remain unaffected.

(3) The invalid or unenforceable provision shall be replaced by a valid and enforceable provision which comes as close as possible to the meaning and purpose of the invalid provision.

(4) For all legal disputes between the parties, the Contractor shall choose the place of jurisdiction.

Appendix
Technical and organisational measures of the contractor (TOM)

1. Confidentiality

>>Access control

No unauthorised access to the contractor's data processing facilities:

- Manual locking system
- Personal control at reception
- Intruder alarm system
- Video surveillance of outside office area
- Careful selection of cleaning staff (cleaning only when present)

>> Access control

No unauthorised use of the contractor's systems:

- Creation of user profiles according to assigned tasks
- Assignment of user rights
- Authentication with user name / password
- Use of passwords in terms of length and complexity according to IT security guidelines
- Assignment of user profiles to IT systems
- Encryption of data carriers in laptops
- Use of a hardware firewall
- Screen lock with password activation

>> Access control

No unauthorised reading, copying, modification or removal within the contractor's systems:

- Differentiated authorisation concepts and needs-based access rights, logging of accesses.
- Administration of rights by IT
- Reduction of administrator roles and their use to the "bare essentials".
- Password policy incl. password length, password change
- Logging of access to critical company applications, especially when entering, changing and deleting data, as far as technically possible
- Proper destruction of data media
- Logging of destruction

>> Segregation control

Separate processing of data collected for different purposes in the client's systems:

- the client's data is kept separate from the data of other clients of the contractor as far as technically possible.

>> Pseudonymisation

Personal data is processed in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that this additional information is stored separately and is subject to appropriate technical and organisational measures;

- not within the scope of the contractor's duties

2. integrity

>> Transfer control

No unauthorised reading, copying, modification or removal during electronic transmission or transport from the Contractor's systems:

- Authentication is encrypted
- As a matter of principle, data carriers are secured during transport, if necessary
- Encryption according to the state of the art

>> Input control

Determination of whether and by whom personal data have been entered, changed or removed from systems:

- Logging of activities

3. availability and resilience

>> Availability control

Protection against accidental or deliberate destruction or loss of data in the contractor's systems:

- Uninterruptible power supply (UPS)
- Air conditioning in server rooms
- Devices for monitoring temperature and humidity in server rooms
- Protective socket strips in server rooms
- Fire and smoke detection systems
- Fire extinguishers in server rooms
- Backup & recovery concept
- Testing of data recovery
- Emergency plan

- Data backup at an external location
- Server rooms not below rooms with sanitary facilities

4. procedures for regular review, assessment and evaluation of the TOM

>> Data protection management

Regular review of the effectiveness of technical and organisational protection measures

- Regular data protection training for employees
- Data protection guideline and work instructions Safeguarding data subjects' rights Informs employees about GDPR requirements

>> Incident response management;

Work instructions for recognising and reporting security incidents / data protection breaches (also with regard to the obligation to report and notify)

- Documentation of security incidents / data protection breaches
- Dummy user account for alerting in case of abuse after a breach

>> Order control

No commissioned processing without corresponding instructions from the client

- Clear and Art.28 GDPR compliant contract design

Formalised order management (ticket system)

- Strict selection of the service provider, obligation to convince in advance

- End -