

# General Terms and Conditions relating to the Applications of Management Services Helwig Schmitt GmbH

## § 1 Scope of Application

The provision of the applications offered by Management Services Helwig Schmitt GmbH ("Management Services") including, without limitation, MIS Sales, MIS After-Sales, OptiNet, MIScubes, MISelements, mobileMIS (collectively „MIS“) and the right of use thereof is subject to these General Terms and Conditions ("GTCs").

These GTCs in their respective version are considered accepted upon conclusion of the Agreement or at the latest by starting to use MIS. These GTCs are the only conditions upon which Management Services is prepared to deal with the Client and they shall govern the Agreement to the entire exclusion of all other terms or conditions. No terms or conditions endorsed upon, delivered with or contained in any documentation from the Client whatsoever shall form part of the Agreement. The Client's terms and conditions do not apply even if Management Services does not expressly contradict them.

These GTCs will also apply when Management Services is aware of terms and conditions of the Client conflicting with or diverging from these GTCs and performs its services without reservation. In these cases the acceptance of the service through the Client triggers the validation of the GTCs and along with this, it cancels the terms and conditions of the Client.

## § 2 Scope of Services, Data Provision

### 2.1 Management Services Obligations:

2.1.1 Management Services shall provide MIS as a web-based browser application. MIS will be hosted on Management Services own servers. Details relating to the technical availability of MIS, in particular to the technical parameters and methods for measuring and determining the availability at the data transfer point (see § 2.2.3) are set out in the Service Level Agreement in Annex 1. In case of any discrepancies between this Agreement and the SLA within the scope of the SLA, the SLA prevails.

2.1.2 Management Services shall provide user credentials (username and related password) to the Client for the log-in to the password-protected area of Management Services website. For this purpose, the Client shall make known to Management Services all intended users who will use MIS and shall also notify within a period of one month of any changes in the assignment of users caused by organisational change, employee changes etc.

2.1.3 Management Services shall provide detailed user documentation on MIS in electronic form to the Client. On request and after consultation with the Client, Management Services shall offer user training for MIS for an additional fee. Management Services reserves the right to subcontract user training to a professional training partner at no additional cost to the Client.

2.1.4 Management Services shall provide a telephone Hotline on weekdays (Monday to Friday) from 8 to 17 local time Hofgeismar, Germany, excluding public holidays in Germany and under normal working conditions. The Client may make inquiries concerning MIS using this hotline.

2.1.5 Management Services shall make every effort to develop and enhance MIS at its own discretion and shall make regular adjustments of MIS for quality maintenance purposes. However, Management Services is under no obligation to the Client to do so. Any specific developments of the standard MIS requested by the Client shall only be provided if this has been expressly agreed in writing.

Management Services reserves the right to implement new versions and upgrades of MIS including, but not limited to, changes

that effect modifications to the design, operational method, technical specifications, systems and other functions etc. of MIS, at any time without prior notice.

2.1.6 In case that OptiNet shall be provided to the Client, Management Services will create a master scenario for planning for the Client at the commencement of this Agreement. This master scenario contains network structures and market data determined by the Client and available to the Client within MIS. Management Services shall make available processed market data updates (see § 2.2.2) for OptiNet on an annual basis. The processing of additional geographic or numerical data will be considered additional services and will incur additional charges. The OptiNet licence includes the web storage space for up to 20 plan scenarios per user. Additional scenarios can be exported and stored locally by the user.

2.1.7 mobileMIS is an optional application for iPhone and/or Android smartphone, which complements MIS. It provides mobile access to market data in a compact format. The range of data is reduced to the essential in comparison to MIS. The data is clearly presented in the form of tables, charts, gauges and portfolio views. Access is provided via an App available for download from the Apple App-Store or Google Play Store. mobileMIS requires a current version of the operating system iOS (minimum iOS 11.0) or Android (minimum Android Nougat (API 24)). mobileMIS can only be used in combination with a current valid MIS licence. The terms and conditions of this Agreement with respect to MIS shall apply mutatis mutandis with respect to mobileMIS.

2.1.8 The geographic point data, including location data of competitor outlet information, boundary data and the entire maps ("Geographic data") as well as the socio-demographic data incorporated into MIS are obtained from external data suppliers or are publicly available. The Client is not entitled to nominate a particular supplier of Geographic and/or socio-demographic data for incorporation into MIS.

The course of boundary lines as well as the position of locations on the map are only approximate and may deviate from their real course or position.

The Geographic and socio-demographic data are updated regularly. Nevertheless, the data does not always correspond to the current state. The Client acknowledges and agrees to the fact that the data is by nature a static representation of a dynamic environment, which automatically has a certain degree of outdated structures.

The calculation of drive time is based on theoretical assumptions and can deviate from actual drive times. Drive times and geographic point references are not capable of being used for navigation purposes.

Locations generated and simulated by OptiNet are based only on selected data available in the system. The algorithms used for this do not reflect all of the circumstances that exist in reality and that would have to be taken into account in a comprehensive site planning.

2.1.9 Assessing the accuracy, completeness and correctness of the data used in MIS [including, without limitation, data provided to Management Services by the Client and/or by others on its behalf (see § 2.2.2) and/or Geographic data and socio-demographic data (see § 2.1.8)] or any material provided by the Client or by others on its behalf (see § 2.2.1) does not constitute a contractual obligation of Management Services.

Management Services is not responsible for capturing the data and/or material on which information or statistics are based and

can only provide information or statistics based on data and/or material as captured by the Client or the relevant authorities, institutions or data providers. The accuracy of information or statistics can therefore not be guaranteed. Management Services assumes that the supplied data and/or material is accurate and provides it to the Client "as is", i.e. in the quality in which it is supplied, without any changes unless otherwise agreed with the Client.

Management Services therefore disclaims all warranties, express or implied, and all responsibilities as to the accuracy, completeness and correctness of the data and/or material used in MIS. In no event will Management Services be liable for any expense, loss or damage including, with-out limitation, indirect or consequential loss or damage, or any expense, loss or damage whatsoever arising from use, or loss of use, of data and/or material, arising out of or in connection with the use of MIS.

Should Management Services find obvious inaccuracies, Management Services shall inform the Client.

## **2.2 Client Obligations:**

2.2.1 It is the responsibility of the Client to ensure that Management Services receives all necessary documents and information in due time for the execution of their tasks and that Management Services is informed of all relevant processes and circumstances. This also applies to documents, processes and circumstances, which become known during the performance of said tasks by Management Services.

2.2.2 Subject to the provisions of § 3.2, the Client shall provide to Management Services free of charge for the duration of this Agreement such data as may be agreed between the parties for Management Services to provide MIS, e.g. internal data [dealer sales, network definitions (locations and areas) and the segment table respectively detailed aftersales data and references like parts references, labour code references and car model references] and, if appropriate, market data [new registrations, ownership transfers (used cars) and vehicle parc (units in operation)]. In case that OptiNet shall be provided to the Client, the Client agrees that Management Services will draw this data required to setup OptiNet from the MIS database of the Client of the respective country. Upon consultation with Client, Management Services will use its best endeavours to acquire the market data annually/periodically, if available, from an external entity, e. g. a public authority or institution or any other data provider, on behalf of the Client and will invoice the total annual cost to the Client when the data is first provided within MIS. The Client shall transfer the required data to process MIS in time, completely and in the file format the Parties have agreed upon (see § 2.2.3) to Management Services and is at all times responsible for its content and quality.

The Client shall retain copies of all documents and data media provided to Management Services, which Management Services can at any time and at no cost resort to. Before sending data and information to Management Services the Client shall check them for malware and use state of the art programs to combat malicious programs.

2.2.3 The Client undertakes to establish a data connection between the workstations intended for its use and the designated data transfer point at Management Services. Unless otherwise agreed, the data transfer point is the network port of the data centres at Management Services that connects to Management Services' Internet Service Providers ("ISP"). Management Services is entitled at any time to redefine the data transfer point, if this is necessary to maintain and/or improve the service quality. The Client shall in this case establish a connection to the newly defined transfer point.

The Parties will agree upon the technical requirements for data exchange as well as the file formats of the data supplied to Management Services by the Client (pursuant to § 2.2.2). Subsequent

amendments thereto are possible only by mutual agreement in writing.

In order to use MIS, certain requirements must be met regarding the customer-side hardware and the web browser used. These will be communicated in advance to the Client by Management Services. Management Services reserves the right to adjust these requirements.

For the avoidance of doubt, Management Services is neither responsible for the quality of the required hardware and software on the side of the Client nor for the telecommunications link between the Client and the transfer point at Management Services.

2.2.4 Management Services reserves the right to invoice the Client for any disadvantages or additional costs resulting from delayed or incorrect data supplied by the Client.

2.2.5 The Client accepts that in the course of using OptiNet the responsible account managers as well as the administrators of Management Services may have access to the planning scenarios created by the Client and as well as to the data which the Client has possibly uploaded. Management Services agrees to treat this information as confidential information according to § 4. When a user access is deleted, all planning scenarios created by the respective user and all data uploaded by the respective user into OptiNet are automatically deleted. To prevent this, the Client can arrange with Management Services to have existing planning scenarios transferred to another user or to have them exported to a data storage media.

## **§ 3 Copyright and Intellectual Property Rights ("IPR"), Rights of Use, Violation of Usage Rights**

### **3.1 Management Services IPR:**

3.1.1 The software, all data, databases, information features, algorithms, forms of visualisation, all other content of MIS and all documents provided by Management Services as part of the Agreement preparation and execution, the Geographic and socio-demographic data and related user documentation (hereinafter "MIS including any Documentation") are protected by copyright and other laws for protection of intellectual property. All rights therein, whether registered or not, which are protected or can be protected and are entitled to Management Services at the time of the completion of this Agreement or are acquired by Management Services as a result of edits, changes or improvements - including after completion of this Agreement - shall, as between the Parties, belong (with the exception of data and/or material provided by the Client according to § 2.2.2 and § 2.2.1) exclusively to Management Services or, alternatively, Management Services shall have the right to use the same. Management Services reserves all copyright and other proprietary rights, including all publication, reproduction, processing and utilization rights to MIS including any Documentation.

3.1.2 Nothing stated herein shall be deemed to grant, transfer, assign or set over to the Client any right, title, interest or ownership of MIS including any Documentation, all of which is expressly reserved by Management Services. There are no implied licences or other implied rights granted under this Agreement, all rights save for those expressly granted hereunder shall remain with Management Services and its licensors.

3.1.3 Management Services grants the Client and its MIS participating franchise dealers (dealers only if opt-in) for the term of this Agreement and for its own internal purposes in the course of business, with regard to the internal data provided by the Client (pursuant to § 2.2.2) a sole right, otherwise a non-exclusive, non-transferable, with the exception of § 3.1.6 non-sublicensable, limited term world-wide right to use MIS including any Documentation in accordance with this Agreement and the documentation by its own personnel. For the avoidance of doubt, the licence granted in this § 3.1.3 shall continue indefinitely beyond the termination or expiration

tion of this Agreement with respect to any reports or other derivatives generated with MIS for the Client during the term of the Agreement according to § 3.1.5.

3.1.4 Components of MIS including any Documentation may include code, libraries, data, databases, information features, algorithms, forms of visualisation or other content licensed by third parties to Management Services, including but not limited to free and open source software (hereinafter "Third-Party Components"). The rights to use these Third-Party Components may be subject to separate licence conditions provided by other copyright holders. The Third-Party Components in MIS are included pursuant to each individual licence and subject to the disclaimers and limitations on liability set forth in each licence and are specifically excluded from all warranty and support obligations described elsewhere in this Agreement.

In the "About-Box" of MIS, Management Services will disclose to the Client the official copyright notices and specific licence conditions of these Third-Party Components, if applicable. The Client agrees to comply with such terms. In addition, the Client will take sole responsibility for obtaining and complying with any licences that may be necessary to use third-party software, data or other materials that the Client uses or obtains for use in conjunction with the use of MIS. The Client acknowledges and agrees that Management Services has no responsibility for, and makes no representations or warranties regarding, such Third-Party Components or the Client's use of such Third-Party Components.

3.1.5 The above-mentioned right of use includes the right to export any reports or other derivatives generated with MIS using MIS export functions (tables, maps, charts) and to use and edit them for the legitimate business purposes of the Client within the Client's own organisation or companies affiliated with the Client as well as the Client's service providers, subject to the confidentiality clause of § 4, provided that the Client shall have no right to publicly disclose such reports or derivatives without the prior written consent of Management Services.

3.1.6 The Client shall be entitled to grant a non-exclusive, non-transferable right to use MIS to the Client's Group companies/affiliates only within the scope of rights and usages, which are set forth for the Client in this Agreement (sublicence). The Client shall be responsible for any misconduct and any non-compliance of the Client's Group companies/affiliates in relation to their use of MIS as to the provisions of this Agreement. However, the Client's Group companies/affiliates shall be made aware by the Client about the rights and duties resulting from this Agreement. Management Services will provide the Client's Group companies/affiliates with access credentials for MIS upon written receipt of a confirmation granting the sublicence and a list of authorised persons.

3.1.7 All other forms of utilization of MIS including any Documentation in whole or in parts, in particular the translation, adaptation, arrangement, any other alteration and any other forms of copying or reproduction and distribution (offline or online) as well as its renting or lending out require the prior written consent of Management Services. The Client shall not disclose, publish, sell, commercialise in any way, transfer, distribute or otherwise reveal MIS including any Documentation to any third party whatsoever, except with Management Services' prior written consent. § 3.1.12 remains unaffected. For the avoidance of doubt, franchise dealers who are not in possession of a valid user licence granting separate dealer access according to § 3.1.3 shall be classified as third parties. The Client shall take reasonable measures to protect MIS including any Documentation from unauthorised access by third parties.

3.1.8 Access to MIS is personalised. Credentials may be used only by the person who has received them in writing from Management Services. The credentials may not be published or passed to third parties. The credentials shall be kept strictly confidential and shall be protected by adequate measures. The password protected section shall be left after each use. The Client agrees to notify Management Services immediately in writing in the event of any unautho-

rised disclosure or use of MIS including any Documentation and/or the credentials and/or any suspicion that MIS including any Documentation and/or the credentials have been made accessible to unauthorised persons of which the Client becomes aware. The Client shall cooperate fully with Management Services to resolve any such unauthorised disclosure or use. The Client is responsible for any and all actions taken using accounts and passwords of the Client.

3.1.9 The Client shall pay a penalty, which is immediately due in the amount of the monthly fee for any unauthorised use of MIS including any Documentation. Management Services reserves the right to block the illegally used user access and to claim damages, in which case the penalty will be deducted from the damages. § 8.2 remains unaffected.

3.1.10 The Client shall upon first request indemnify and hold harmless Management Services and its licensors from and against any and all claims, liabilities, losses and expenses, including reasonable attorneys' fees, arising out of the Client's use of MIS including any Documentation in breach of the terms of this Agreement. This indemnity is given subject to the indemnified Party giving to the indemnifying Party immediate and complete control of the claim; not prejudicing the indemnifying Party's defence of the claim; and giving the indemnifying Party all assistance reasonably requested by the indemnifying Party in connection with the claim.

3.1.11 Copyright notices or notices on other intellectual property rights, which are located on or in MIS including any Documentation or portions thereof, or any other materials of Management Services, may neither be altered, nor removed, nor otherwise rendered unrecognisable.

3.1.12 The Client is entitled to save, print and for the purposes of exercising its rights under this Agreement to reproduce in adequate numbers the available user documentation while adhering to existing copyrights notices.

3.1.13 The source code of MIS is not provided by Management Services, nor published or filed with a third party.

3.1.14 The processing and/or reconciliation of the data within MIS with other datasets, which could result in a possible de-anonymisation or re-identification is not permitted. It is also not allowed to use the data for the purpose of individual credit checks or credit scoring.

3.1.15 The MIS may contain hyperlinks to third-party websites. Management Services neither accepts any responsibility for the content of such websites nor does Management Services make these websites and their content its own because Management Services does not review the linked information and is not responsible for the content or information held there. The Client uses these at his own risk.

3.1.16 The foregoing provisions shall apply mutatis mutandis to new releases, updates, upgrades or other new versions of MIS including any Documentation as available during the term of this Agreement.

### 3.2 Client IPR:

3.2.1 The Client retains whatever ownership or rights it may have in the data and/or in any material in any form provided by the Client (see § 2.2.2 and § 2.2.1) and nothing in this Agreement transfers any ownership to Management Services in said data and/or material. The Client grants Management Services the right to use the data and/or material to the extend necessary to perform the services to the Client, i.e. to use, process, create derivative work of and display the data and/or material, for the duration of this Agreement.

3.2.2 By submitting data and/or material to Management Services the Client is certifying that the Client is the originator of the data and/or any material and has not copied any information, which is subject to the copyright of another organisation or individual, or the Client is certifying that the Client has the authority to submit this information to Management Services under the terms stated here.

3.2.3 The Client shall upon first request indemnify and hold harmless Management Services from and against any and all claims, liabilities, losses and expenses, including reasonable attorneys' fees, arising out of any third-party claims for infringement of third-party rights (including but not limited to intellectual property rights and/or data protection rights) arising out of the data and/or the material which the Client provides to Management Services for the fulfilment of the services. This indemnity is given subject to the indemnified Party giving to the indemnifying Party immediate and complete control of the claim; not prejudicing the indemnifying Party's defence of the claim; and giving the indemnifying Party all assistance reasonably requested by the indemnifying Party in connection with the claim.

#### § 4 Confidentiality

4.1 Confidential information includes all information and documents, including this Agreement, from either Party, which are either marked as confidential or their confidentiality stems from the circumstances or its nature. In addition, confidential information is that which would be considered worthy of protection and therefore should be treated as confidential by knowledgeable third parties. Confidential information includes in particular business and company secrets, technical, business, and other information, for example information relating to technologies, products, services, discoveries, inventions, concepts, designs, documentation, pricing, customers, employees, strategies. Considered confidential are on the one hand the underlying data and all information contained in MIS including any Documentation including credentials and on the other hand data delivered by the Client, which are required for the evaluation, modifications, enhancements and maintenance of MIS.

4.2. Not considered confidential information is information which  
a) is known to the receiving Party before received from the other Party in connection with this Agreement;

b) the receiving Party has developed independently without resorting to confidential information of the other Party;

c) was acquired by the receiving Party from third parties and which is not bound by restrictions with respect to its use and disclosure;

d) without fault or intervention of the receiving Party is or becomes generally known.

4.3. The Parties shall keep secret any confidential information, which one Party has communicated to the other Party or has received from the other Party under this Agreement. They shall protect confidential information from unauthorised access and treat it with the same care they apply to their own, equally confidential information, and at least with the diligence of a prudent businessman. Confidential information may only be disclosed to employees of the respective contracting Party and this only if the employees concerned either belong to the authorised user group of the Client or the disclosure is necessary for the performance of this Agreement ("need to know"). These employees shall be bound to secrecy on the basis of a contractual agreement.

4.4. Confidential information may not be disclosed by the receiving Party to third parties without the prior written consent of the other Party, unless

a) this is due to compelling legal requirement or required by a court or official order, and the receiving Party has immediately informed the other Party in writing of the respective obligation and given it the opportunity to take action against the disclosure, or

b) the confidential information is made available to third parties within the scope of the permitted usage pursuant to § 3.1.5 or to the service provider of the receiving Party in connection with the execution of this Agreement (e.g. auditors, tax advisors, banks, insurances, with the exception of competitors of Management Services) and the third party and/or the service provider has previously agreed to confidentiality with the receiving Party, in writing, or is bound to a professional obligation to maintain confidentiality.

4.5. When the Agreement ends, the Parties shall return to each other the confidential information received from the other Party or destroy it in an appropriate manner. As an exemption hereto, data received from the Client according to § 2.2.2 shall not be returned to the Client by Management Services neither in raw nor in processed format but rather destroyed by Management Services. Management Services will certify the destruction of such confidential information or data upon request.

Excluded from this regulation are cases where the Parties are obliged to archive the other Party's confidential information due to compelling commercial or tax law provisions as well as if there are reasonable grounds to believe that its destruction could affect the legitimate interests of the affected Party, e.g. for purposes of providing proof of their own legal claims.

4.6. Subject to further confidentiality obligations due to mandatory legal requirements, this obligation of confidentiality continues to exist for three years after termination of this Agreement.

4.7 The Client agrees that Management Services may use the Client's name and logo as part of the company's customer reference list and to make them available to third parties for information.

#### § 5 Data Protection

5.1 Management Services shall process the personal data provided by the Client on behalf and in accordance with the instructions of the Client within the meaning of Art. 28 General Data Protection Regulation (2016/679), ("GDPR"), (processing on behalf). The Client remains the controller in terms of data protection law. Details are set out in a separate Data Processing Agreement (see Annex 2).

5.2 Both Parties agree to comply with the applicable data protection legislations and regulations, including, (i) the GDPR, (ii) the national laws implementing the Directive on Privacy and Electronic Communications and (iii) any other regulations effective that may apply to Personal Data processed in the course of the performance of this Agreement. Both Parties shall ensure that all persons entrusted with the performance of this Agreement observe the statutory provisions on data protection. They shall especially obligate their employees to maintain confidentiality in accordance with the requirement to observe special instructions relating to data processing.

5.3 When the Client processes personal data itself or through Management Services, the Client is responsible for ensuring that the Client and/or Management Services are entitled to do so under the applicable regulations and in particular under the applicable data protection laws.

5.4 The data sent by the Client to Management Services (see § 2.2.2) has to comply with data protection laws especially relating to data minimisation and pseudonymisation. The Client shall send to Management Services only the data required to carry out this Agreement.

#### § 6 Delivery and Delays

6.1. Details on the delivery date are non-binding. Binding delivery dates need the written approval of Management Services. Partial deliveries shall be permissible.

6.2 Periods of delivery and service shall be extended by a period of time during which Management Services waits for information or cooperation acts of the Client.

#### § 7 Prices and Terms of Payment, Set-off and Assignment, Taxation

7.1 Payments are due within 30 days upon receipt of the invoice and the delivery without deduction.

7.2 The fees paid under this Agreement are exclusive of all Taxes, as defined herein. The Client will pay all taxes or other charges levied in connection with the services rendered by Management Services,

including without limitation import or export fees, duties, sales, services, use and value-added taxes, withholding taxes or similar charges (collectively, "Taxes") which are imposed by or under the authority of any government or any political subdivision thereof, excluding taxes based upon Management Services' net income. The Client will be responsible for complete and clearance of such tax filing or payment procedures.

All payments due from the Client shall be made without any deduction or withholding on account of any Taxes, charge or penalty, except required by law, in which case the sum payable by the Client from which such deduction or withholding is to be made shall be increased to the extent necessary to ensure that, after making such deduction or withholding, Management Services receives and retains (free from any liability with respect thereof) a net sum equal to the sum which Management Services would have received had no such deduction or withholding been made or required to be made.

The aforementioned section does not apply if the Client provides Management Services within 60 days of the Client's payment with documentation and proof of any Taxes paid on the services rendered by Management Services. The Client shall furnish evidence of such paid Taxes as is sufficient to enable Management Services to obtain any credits available to it, including original withholding tax certificates.

7.3 The invoice issued by Management Services includes the VAT/Turnover Tax Identity Number provided by the Client (if EU) to Management Services. Where an incorrect VAT/Turnover Tax Identity Number is given, the Client is liable towards Management Services for the tax liability claimed from Management Services by the tax authorities.

7.4 Only where the Client's claims have legal force or are uncontested shall the Client be entitled to set-off or assert a right of retention against counterclaims of Management Services. The Client shall not assign claims against Management Services without the prior written approval of Management Services.

7.5 If the Client orders services under this Agreement to be performed at a location other than Management Services' offices, the Client will reimburse Management Services for all reasonable travel-related expenses incurred by Management Services including, without limitation, transportation, lodging, and meal expenses.

7.6 Management Services reserves the right to negotiate with the Client a price adjustment if the prices of the data used in MIS unexpectedly rise by more than ten percent relative to the price agreed between Management Services and the external data providers at the time of the conclusion of the Agreement. If the Parties cannot agree in this case, each Party is entitled to terminate this Agreement for exceptional reasons in writing. In this case, Management Services is entitled to remuneration for services rendered up to the effective date of termination under the Agreement.

## § 8 Term and Termination

8.1 The Agreement shall commence on the Effective Date as agreed between the Parties. The Agreement shall run for an initial minimum term of 24 months. It shall be automatically renewed for additional 12 months periods unless either Party requests termination at least six (6) months prior to the end of the initial or any subsequent term. Notwithstanding the commencing date of this Agreement, these rules apply *mutatis mutandis* for the term and termination notice of markets and dealer accesses. Termination of a single dealer access due to any changes in the assignment of users caused by organisational change, employee changes etc. may be accepted with a shorter notice period.

8.2 Notwithstanding the aforementioned § 8.1, either Party shall be entitled to terminate this Agreement with immediate effect – without termination or notice period - forthwith by written notice to the other Party if:

a) the other Party commits a severe material breach of this Agreement which is not capable of being remedied or which is capable of being remedied but which it fails to remedy within 21 days of notice from the other Party requiring remedy of such breach; or

b) the other Party commences (or considers commencing) insolvency proceedings (or similar) or becomes insolvent.

8.3 Each notice shall be given by registered mail.

8.4 The access to MIS expires at the end of the term of this Agreement.

## § 9 Limited Warranty, Defects and Shortcomings

9.1 In the current state of the art, with complex software products such as MIS the occurrence of program errors cannot be completely excluded. The agreed quality of MIS is therefore not that no program error may occur or that MIS can be used for every conceivable application. The agreed quality is that MIS will perform substantially and materially in accordance with its documentation, under normal use and circumstances, and for the purpose intended and that it has no bugs that could more than only negligibly affect the intended usability such that said performance is no longer acceptable under reasonable conditions.

Except for the express warranties set forth above and to the extent permitted by law, Management Services expressly disclaims all other warranties with respect to MIS including any Documentation, whether express or implied, including without limitation, merchantability and fitness of MIS for a particular purpose, accuracy or reliability of results from use of MIS, that MIS will meet the individual needs and specific requirements of the Client, that MIS will be uninterrupted, completely secure, free of software errors, or that defects and deficiencies will be corrected. Statements and presentations in trial versions as well as in product and project specifications do not constitute guarantees for MIS including any Documentation; such guarantees require express written confirmation from Management Services.

Management Services does not guarantee that MIS is particularly suitable for specific commercial evaluation by the Client. The Client understands and agrees that Management Services does not warrant that the forecasts, projections, advice, recommendations or any other content in MIS will be accurate or achievable. Future decisions may depart from historical practices, which have been considered in the algorithms. Although the algorithms have been tested and validated, Management Services is not privy to manufacturers' strategic decision making. Because of the uncertainty of future events and circumstances, and because the content in MIS is based on data and information provided by the Client and/or third parties, upon which Management Services has relied upon in good faith in producing MIS, the nature of the data and information in MIS is such that it is not appropriate for the Client or any other person to make commercial decisions based solely on that information. Accordingly, the Client understands and agrees that Management Services is not liable for any actions taken or not taken based on the content of MIS. Insofar as MIS is used to support business decisions by the Client, Management Services does not assume responsibility either for the decision itself or any commercial or legal risks resulting thereof. Furthermore, as Management Services is not allowed to give legal or tax advice, the Client is obliged to make certain, that all the necessary requirements in connection herewith are fulfilled.

9.2 For the avoidance of doubt, the transfer of the data to be supplied by the Client to Management Services (see § 2.2.2) takes place solely at the risk of the Client. Delays, losses or changes to data during this transfer until it is received by Management Services do not constitute any rights of the Client to claim defect. Management Services is also not liable for the quality of the raw data used for evaluation in the MIS. Management Services does not warrant nor guarantee a certain timeliness or accuracy of the data unless expressly stated in the product description or otherwise agreed.

9.3 The Client shall inform Management Services in writing immediately, at the latest within two weeks, if the Client recognizes that Management Services has not performed a service in accordance with this Agreement. The Client must specify the non-contractual provision of services to Management Services in as much detail as possible. Failure to comply with this regulation will invalidate the warranty regarding the provision of services.

9.4 Regarding defects and shortcomings concerning the technical availability of MIS the Service Level Agreement in Annex 1 applies exclusively. Under technical availability the Parties understand the availability of MIS for access and use by the Client through an Internet connection at the data transfer point (see § 2.2.3). For all other defects and shortcomings, the following provisions of this § 9 shall apply.

9.5 In the case of major material defects that seriously impede the Client's use of MIS and that are attributable to Management Services, Management Services undertakes to act to rectify such defect within a reasonable period of time.

Insofar as Management Services is responsible for the inaccuracy, incompleteness or irregularities of the data used in MIS due to its own actions, Management Services shall rectify this data promptly and make them available to the Client.

In the case of legal defects for which Management Services is responsible, Management Services shall at its option, either

- a) procure for the Client the right to continue the use of MIS, or
- b) replace MIS with non-infringing services of materially equivalent function and performance, or
- c) modify MIS so that it becomes non-infringing without materially detracting from its function.

9.6 Should none of these measures be technically, commercially or economically reasonable to Management Services or fail in substantial parts, for reasons that Management Services is responsible for, even within a reasonable period of grace set by the Client and despite at least two repair attempts on the part of Management Services, then either Party may terminate the Agreement for good cause without notice. Alternatively, the Client is entitled to reduce the contractual remuneration for the duration of the existence of the defect to a maximum of 30%. In the case of termination, Management Services is entitled to remuneration for services rendered under the Agreement up to the effective date of termination. A right of cancellation does not apply to minor defects.

9.7 In the absence of intent or gross negligence by Management Services or injury to life, body or health, Management Services otherwise assumes no responsibility for defects or deficiencies in MIS including any Documentation. Further claims based on improper provision of services are excluded.

9.8 The above claims under this § 9 shall expire within one year from the commencement of the statutory limitation period. This does not apply in cases of intent or gross negligence on the part of Management Services, its legal representatives or vicarious agents, and to the injury of life, body or health, or to the liability under the Product Liability Act. In these cases, the statutory limitation period applies.

## § 10 Liability

10.1 In cases of violation of contractual obligations, or of tort, or of violations based on other legal standpoints, the liability of Management Services, its legal representatives and its vicarious agents, shall be limited to cases of intent or gross negligence, while in cases of violation of a cardinal contractual obligation (essential contractual obligation) the liability of Management Services shall be limited to damage typical of the Agreement and foreseeable at the time of conclusion of the Agreement.

10.2 The Client is responsible for the regular backup of data according to the state of the art (at least once a day on an external data

memory) and ensures that the data kept in machine readable format are data sets reproducible with reasonable efforts. Should Management Services be responsible for loss of data, Management Services is only liable pursuant to this § 10 for the expenditure incurred to restore the data from these proper backups by the Client.

10.3 In the event of injury to life, body or health, or as part of a liability under the Product Liability Act, the liability of Management Services is unlimited.

10.4 Strict liability on the part of Management Services for defects already in existence at the time of the conclusion of this Agreement (§ 536 a BGB, German Civil Code) is expressly excluded.

10.5 The above liability claims shall expire within one year from the commencement of the statutory limitation period. This does not apply in cases of intent or gross negligence on the part of Management Services, its legal representatives or vicarious agents and to the injury of life, body or health or to the liability under the Product Liability Act. In these cases, the statutory limitation period applies.

## § 11 Trial-/Demo-versions

11.1 If MIS is provided for testing or demonstration purposes, resp. as "Trial-/Demo-Version", same is not associated with the granting of a right of use, but only acceptance of use for the purposes concerned for the agreed or a reasonable period, which can be revoked at any time. The acceptance of use ends automatically when the Client violates the terms and conditions.

11.2 Trial versions of MIS are not intended for productive operation but only for test purposes. In light of the fact, that trial-versions are provided free of charge, they are provided "as is". The use is at the Client's own risk.

11.3 Management Services disclaims all warranties, representations and liabilities as set forth in this Agreement and Management Services shall not be liable for damages of any kind related to the Client's use of a trial-version. This rule does not apply in cases of intent or gross negligence on the part of Management Services.

## § 12 Trainings and workshops

12.1 Trainings and workshops can be cancelled by the Client free of charge up to 30 days before the start. For cancellations up to 14 days before the start date 50% of the cost will be charged. In the case of a cancellation after this date, 100% of the agreed price as well as possibly already incurred travel costs will be charged.

12.2 Management Services reserves the right to cancel or reschedule trainings and workshops in the event of non-availability of the instructor (in particular due of illness), force majeure, or for important other reasons that are beyond Management Services' control.

## § 13 Force Majeure

Neither Party shall be liable for any delay or failure in performance (other than for delay in the payment of amounts due and payable hereunder and the maintenance of confidentiality) due to Force Majeure, which shall mean, inter alia, acts of God, earthquake, labour disputes, changes in law, regulation or government policy, riots, war, fire, epidemics, acts or omissions of vendors or suppliers, terrorism, power failures, errors in another operator's network, internet interruptions, transportation difficulties or other occurrences which are beyond a Party's reasonable control. Technical internet problems that result in server malfunction, as well as any failures caused by illegal invasion (i.e. hacking attacks) that could not have been prevented by technically and economically reasonable measures, are also to be considered as Force Majeure provided that they are not influenced by one of the Parties. If contractual obligations cannot be fulfilled, either in a timely fashion or otherwise as agreed due to Force Majeure, the respective contractual Party shall be released from its obligation to perform according to the scope

and duration of the Force Majeure effect including a reasonable recovery phase. The Parties shall inform each other immediately of the events of Force Majeure.

#### § 14 Final provisions

**14.1 (Variation)** Any alterations, modifications, amendments or supplements to this Agreement must be in writing and signed by both Parties. Even a change to the written form requirement requires the written form in order to be valid.

**14.2 (Severance)** In the event that any provision of this Agreement or part of it should be or become invalid, the validity of the other provisions of this contract shall not be affected here-by. The invalid provision shall be replaced by a valid provision, which in particular comes closest to the economic intent of the Parties. The same applies in case of a loophole in the Agreement that must be closed.

**14.3 (Status)** This Agreement constitutes the entire agreement between the Parties regarding the subject matter hereof and supercedes any and all prior negotiations, promises, commitments undertakings and agreements of the Parties relating thereto. General Terms and Conditions of the Client shall not apply even if Management Services does not expressly contradict them. Any term(s) contained in the Client's purchase order, acknowledgement form or any other form that is different from, or in addition to this Agreement, shall not have any effect of modifying or adding any terms to the Agreement and shall be for the Client's internal purpose only.

**14.4 (Waiver)** No omission or delay by either Party at any time to enforce any right or remedy reserved to it, or to require performance of any of the terms, covenants or provisions here-of at any time designated, shall be a waiver of any such right or remedy to which either Party is entitled, nor shall it in any way affect the right of either Party to enforce such provisions thereafter.

**14.5 (Costs)** Each Party shall bear its own costs in connection with the preparation and execution of this Agreement.

**14.6 (Relationship of the Parties)** This Agreement is not intended to and shall not render any employee of Management Services as an employee of the Client and the Client shall not hold itself out as such. This Agreement shall not constitute either Party the agent of the other, or create a partnership, joint venture or similar relationship between the Parties, and neither Party shall have the power to obligate or bind the other in any manner whatsoever. In all respects, each Party shall act at all times as an independent contractor for all purposes of this Agreement.

**14.7 (Disputes)** In the event of any dispute relating to this Agreement, the Parties agree to initially make a full and good faith attempt to resolve such dispute by negotiation at an executive level, to the extent reasonable under the circumstances, prior to commencing court proceedings.

**14.8 (Place of Performance)** The place of performance shall be the registered office of Management Services.

**14.9 (Place of Jurisdiction)** Place of jurisdiction shall be Kassel, Germany.

**14.10 (Governing Law)** The contractual relationship shall be subject to the laws of the Federal Republic of Germany with the exception of its conflict of law provisions and the UN Sales Convention (United Nations Convention on Contracts for the International Sale of Goods dated 11.4.1980 Agreement).

**Status: January 2023**

## Service Level Agreement

### 1. Availability Objective:

Management Services will provide 99,9 % Availability (as defined below) for Software within Management Services' Immediate Control. For purposes hereof, "Availability" or "Available" means the Software is available for access and use through an Internet connection at the data transfer point. Capitalized terms used in this Service Level Agreement ("SLA") but not defined herein shall have the meanings given in MIS-Agreement (the "Agreement").

#### 1.1 Immediate Control

"Immediate Control" includes all components below:

- (a) Management Services' network services within the Management Services' data centres which terminate at Management Services' Internet Service Providers ("ISPs") (i.e., public Internet connectivity);
- (b) Hardware provided by Management Services and managed at the Management Services' data centre.

Specifically excluded from the definition of "Immediate Control" are the following:

- (a) Equipment, data, materials, software, hardware, services and/or facilities provided by or on behalf of the Client and the Client's network services, which allow the Client to access the Software. These components are controlled by the Client and their performance or failure to perform can impair or disrupt the Client's connections to the Internet and the transmission of data.
- (b) Equipment, data, materials, software, hardware, services and/or facilities provided by third-party vendors or service providers of the Client.
- (c) Acts or omissions of the Client, its employees, contractors, agents or representatives, third-party vendors or service providers of the Client or anyone gaining access to Management Services' network at the request of the Client.
- (d) Issues arising from bugs or other problems in the software, firmware or hardware of third parties.
- (e) Delays or failures due to circumstances beyond Management Services' reasonable control that could not be avoided by its exercise of due care including a Force Majeure Event.
- (f) Any outage, network unavailability or downtime outside the Management Services' data centre.

#### 1.2 Maintenance Window Scheduled Downtime:

Management Services has an optional "Maintenance Window" on every third Tuesday of the month, during which maintenance, upgrades and repair can occur. In addition to the standard scheduled Maintenance Window, Management Services may require additional scheduled downtime from time to time. Management Services shall plan this schedule for off-peak hours between Saturday 6 a.m. and Sunday 12 p.m. (CET/CEST). This window may contain several hours without service. Management Services will notify the Client one week in advance of any scheduled maintenance where possible. All planned downtime, including the standard Maintenance Window and the scheduled down time, are excluded from the SLA availability calculation.

#### 1.3 Emergency Maintenance:

Management Services will carry out maintenance on an emergency basis to ensure SLA's are maintained. This maintenance will be undertaken at Management Services discretion. Management Ser-

vices will notify the Client of the maintenance where possible. Unavailability due to Emergency Maintenance is excluded and does not count towards unavailability calculation.

#### 1.4 Availability Calculation:

Availability is based on a monthly (28/29/30/31 days x 24 hours) calculation excluding scheduled downtime. Specifically excluded from the Availability measurement are (1) all planned down time including the standard Maintenance Window and the other scheduled down time as well as Emergency Maintenance; (2) a service interruption caused by a security threat until such time as the security threat has been eliminated; (3) reasons of a Force Majeure Event (as defined in the Agreement) or events which are outside Management Services' Immediate Control as defined above; (4) use of unapproved or modified hardware by or on behalf of the Client software; and/or (5) issues arising from misuse of the Services by the Client or its agents, customers or third-party contractors.

#### 1.5 Remedies:

The remedies stated in this section are the Client's sole and exclusive remedies and Management Services' sole and exclusive obligations for service interruption. In the event that Management Services is unable to provide the Availability Objective in any given calendar month, the Client will receive a credit on their next monthly invoice equal to the pro-rated monthly fee.

The Client's right to receive credit(s) will be the Client's exclusive remedy for Management Services' failure to satisfy the SLA. Remedies will not accrue (i.e., no credits will be issued and a downtime will not be considered as unavailability for purposes of this SLA) if the Client is not current in its payment obligations either when the downtime occurs or when the credit would otherwise be issued. To receive service credits, the Client must contact Management Services' support with the request within 8 days after the end of the month in which the service was unavailable, or the Client's right to receive service credits with respect to such unavailability will be waived.

Where a Force Majeure Event prevents full Availability for more than twenty (20) consecutive days in any six (6) month period, the Client's sole remedy is to terminate the Agreement on thirty (30) day's written notice to Management Services. In such case, neither party will be liable for penalties or damages arising out of a failure to perform due to the Force Majeure Event.



**2. Customer Software Support:**

All Maintenance and Support Services will be provided via telephone helpline and via email support@manserv.com, during the hours of 8 a.m. - 5 p.m. (CET/CEST), Monday-Friday, excluding bank holidays in Germany (“Standard Maintenance and Support Times”).

Management Services has structured a response plan to address the most critical issues first. Cases will be opened upon receipt of request or identification of issue, and incidents will be routed and addressed according to the following:

Severity Level	Error State Description	Target Response Time	Target Resolution Time
1 Critical Priority	Renders Software inoperative, or causes to fail catastrophically	2 hours	8 hours
2 High Priority	Affects the operation Software and materially degrades Customer’s use thereof	4 hours	24 hours
3 Medium Priority	Affects the operation of Software but does not materially degrade Customer’s use thereof	24 hours	--
4 Low Priority	Causes only a minor impact on the operation of Software	48 hours	--

**2.1 Errors:**

**(a) Error Definition:** Subject to the terms of the Agreement, Management Services will use commercially reasonable efforts to remedy any failure of the Software which causes the Software to be inoperable or to materially fail to conform to the functional specifications for the Software described in the applicable Documentation published by Management Services (each defined as “Error”) provided that it is reported to Management Services by the Client in accordance with this SLA, and that Management Services is able to reproduce and demonstrate the Error in the environment for which the Software was designed to operate.

Any failure of the Software resulting from the Client’s negligence or use of the Software not in accordance with the applicable user documentation provided by Management Services, breach by the Client of the Agreement or in combination with any third-party soft-

ware other than the software recommended by Management Services will not be considered an Error for which Management Services will be responsible for any corrective efforts.

**(b) Error Reporting:** The Client will report any Errors by sending an email to support@manserv.de. Management Services will have no obligation to respond to or remedy any Error not reported to Management Services in accordance with the terms herein.

**(c) Error Response:** Upon receipt of notification of an Error by the Client in accordance with this SLA, Management Services will confirm the classification of the Error or, when necessary, re-classify the Error appropriately. Management Services will exercise reasonable efforts to resolve the Error in accordance with the applicable Target Resolution Time set forth in the chart above. The Target Resolution Times will begin to run during Standard Maintenance and Support Times (as defined above) once an Error is reported to Management Services in accordance with this SLA.

**2.2 Updates and Upgrades:**

Subject to the terms of the Agreement, including, without limitation, the payment of all fees due thereunder, Management Services may from time to time make available certain minor releases of the Software, including, for example, bug fixes, error corrections and minor enhancements of and to the Software (collectively, “Updates”). Management Services may also from time to time release new versions of the Software having significant enhancements in features, performance or functionality (collectively, “Upgrades”) or entirely new software products (“New Products”). Management Services will determine, in its sole discretion, whether any subsequent version of the Software is an Upgrade, Update or New Product. Management Services will make available to the Client all Updates and Upgrades (but not New Products) that Management Services makes generally available to other clients. New Products will be made available to the Client only under a separate licence Agreement for which a separate fee may be required. Management Services is under no obligation to release any Updates, Upgrades or New Products, or to modify the Software to operate on any updated versions of operating systems or platforms. However, along with the standard release-cycle of Management Services’ standard software, regular updates for operating system and platform support will be provided to keep up with state and advancement of technology.

**2.3 Limitations:**

Management Services is not required to provide any Maintenance and Support Services relating to problems arising out of any use of the Software in a manner not specified in the Documentation and the Agreement.

**3. Customer’s Responsibilities:**

The Client is exclusively responsible for the supervision, management, backup, security, and control of all aspects of the Client’s information technology systems and storage of the Client Content beyond standard storage periods. The Client will provide Management Services with full, good faith cooperation and such information as may be required by Management Services in order to perform the support services.

## Data Processing Agreement

### Recitals

Where processing is to be carried out on behalf of a Controller the processing shall be subject to the current data protection laws, especially in such a manner that processing will meet an appropriate data protection level. This Agreement complies with the special requirements of the General Data Protection Regulation (GDPR), (Regulation (EU) 2016/679) and is supplementary to an agreement entered into between the Client and Management Services Helwig Schmitt GmbH (the "Main Agreement"). For the avoidance of doubt definitions and expressions referred to in this Agreement shall have the same meaning as those set out in the Main Agreement.

In accordance with the above objective, the Client (Controller) and Management Services Helwig Schmitt GmbH (Processor) have agreed as follows:

### § 1 Subject Matter of the Agreement

1.1 The Controller assigns the Processor the task of processing personal data.

1.2 The subject matter of the present data processing Agreement and thus purpose, type and extent of the data collection is the data processing and data evaluation in connection with the Market Information Systems and Consulting Services of the Processor.

1.3 The undertaking of the contractually agreed data processing is carried out exclusively within the territory of the Federal Republic of Germany, a Member State of the European Union or another contracting member state of the European Economic Area. Any transfer to a third country requires the specific authorisation from the Controller and may be carried out provided the fact that the specific conditions of Article 44 et seq. GDPR have been fulfilled.

### § 2 Duration of the Agreement

The duration of the present Agreement corresponds to the Main Agreement and for the avoidance of doubt, the present Agreement shall determine automatically only once the personal data held by the Processor has been destroyed or returned to the Controller in accordance with the Main Agreement.

### § 3 Nature of the Data

The subject matter of the processing of personal data covers the following types/categories of data (list/description of categories of data) of the relevant category of data subjects:

#### MIS Sales and AfterSales/ OptiNet:

##### Data subjects

User of the system:

- Employees, directors and/or other agents of the Controller and/or its affiliates/group companies
- contractual partners of the Controller and their employees, directors and/or other agents (e.g. dealer outlet)
- other partner companies of the Controller and their employees, directors and/or other agents (e.g. suppliers, subcontractors, consultants, temporary employment agencies)

##### Data categories:

- contact data: family name, first name, address data, e-mail address
- IT usage data (log-files: IP-address, client ID, roles, log-times)
- job title
- contract data

**MIS After-Sales** in addition:

##### Data subjects:

Vehicle owner, in part interested parties/prospective buyers

##### Data categories:

- vehicle identification number (VIN), plate number and vehicle information
- vehicle registration data/ car parc data/ ownership transfer data/ cancellation data
- name, job title
- contact data
- address data
- workshop visit and corresponding activities e.g. over the counter sales
- payment and settlement data
- contract data

### § 4 Technical and organisational measures

4.1 Before the commencement of processing, the Processor shall document the execution of the necessary Technical and Organisational Measures, set out in advance of the awarding of the Order or Contract, specifically with regard to the detailed execution of the Agreement, and shall present these documented measures to the Controller for inspection/audit/review. Upon acceptance by the Controller, the documented measures become the foundation of the Agreement (see Annex 3). Insofar as the inspection/audit/review by the Controller of such proposed Technical and Organisational Measures shows the need for amendments, such amendments shall be implemented by mutual Agreement.

4.2 The Processor shall establish the security in accordance with Article 28 section 3 point c, and Article 32 GDPR in particular in conjunction with Article 5 section 1, and section 2 GDPR. The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. The state of the art, implementation costs, the nature, scope and purposes of processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 section 1 GDPR must be taken into account.

4.3 The Technical and Organisational Measures are subject to technical progress and further development. In this respect, it is permissible for the Processor to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced. Substantial changes must be documented.

### § 5 Rectification, Restriction and Erasure of Data

5.1 The Processor may not on its own authority rectify, erase or restrict the processing of data that is being processed on behalf of the Controller, but only on documented instructions from the Controller. Insofar as a Data Subject contacts the Processor directly concerning a rectification, erasure, or restriction of processing, the Processor will immediately forward the Data Subject's request to the Controller.

5.2 Insofar as it is included in the scope of services, the erasure policy, 'right to be forgotten', rectification, data portability and access shall be ensured by the Processor in accordance with documented instructions from the Controller without undue delay.

## § 6 Supervision and Responsibilities of the Processor

In addition to complying with the rules set out in this Agreement, the Processor shall comply with the statutory requirements referred to in Articles 28 to 33 GDPR; accordingly, the Processor ensures, in particular, compliance with the following requirements:

- a) Appointment of a Data Protection Officer, who shall perform his/her duties in compliance with Articles 38 and 39 GDPR. His/Her current contact details are always available and easily accessible on the website of the Processor.
- b) Confidentiality in accordance with Article 28 section 3, sentence 2 point b, Articles 29 and 32 section 4 GDPR. The Processor entrusts only such employees with the data processing outlined in this Agreement who have been bound to confidentiality and have previously been familiarised with the data protection provisions relevant to their work. The Processor and any person acting under its authority who has access to personal data, shall not process that data unless on instructions from the Controller, which includes the powers granted in this Agreement, unless required to do so by law.
- c) Implementation of and compliance with all Technical and Organisational Measures necessary for this Agreement in accordance with Article 28 section 3, sentence 2, point c, Article 32 GDPR [details in Appendix 1].
- d) The Controller and the Processor shall cooperate, on request, with the supervisory authority in performance of its tasks.
- e) The Controller shall be informed by the Processor immediately of any inspections and measures conducted by the supervisory authority, insofar as they relate to this Agreement. This also applies insofar as the Processor is under investigation or is party to an investigation by a competent authority in connection with infringements to any Civil or Criminal Law, or Administrative Rule or Regulation regarding the processing of personal data in connection with the processing of this Agreement.
- f) Insofar as the Controller is subject to an inspection by the supervisory authority, an administrative or summary offence or criminal procedure, a liability claim by a Data Subject or by a third party or any other claim in connection with the Order or Contract data processing by the Processor, the Processor shall make every effort to support the Controller.
- g) The Processor shall periodically monitor the internal processes and the Technical and Organisational Measures to ensure that processing within his area of responsibility is in accordance with the requirements of applicable data protection law and the protection of the rights of the data subject.
- h) Verifiability of the Technical and Organisational Measures conducted by the Controller as part of the Controller's supervisory rights referred to in § 8 of this Agreement.

## § 7 Subcontracting

7.1 Subcontracting for the purpose of this Agreement is to be understood as meaning services, which relate directly to the provision of the principal service. This does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services 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 equipment. The Processor shall however, be obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of the Controller's data, even in the case of outsourced ancillary services.

7.2 The Controller agrees to the commissioning of the following subcontractors on the condition of a contractual agreement in accordance with Art. 28 sections 2-4 GDPR.

Company subcontractor	Address/country	Service
Microsoft Ireland Operations Ltd.	The Atrium Building, Block B, Carmanhall Road, Sandyford Business Estate, Dublin 18, Ireland	Microsoft Diagnostics und Microsoft Analytics of Visual Studio App Center (only mobileMIS).

7.3 Outsourcing to further subcontractors or changing the existing subcontractors are permissible when:

- a) The Processor submits to the Controller a formal notification in writing or in text form of such an outsourcing to the Controller in advance of any such subcontracting; and
- b) The Controller has not objected to the planned outsourcing in writing or in text form by the date of handing over the data to the Processor; and
- c) The subcontracting is based on a contractual agreement in accordance with Article 28 sections 2-4 GDPR.

7.4 The transfer of personal data to the subcontractor and the subcontractors commencement of the data processing shall only be undertaken after compliance with all requirements has been achieved.

7.5 If the subcontractor provides the agreed service outside the EU/EEA, the Processor shall ensure compliance with EU Data Protection Regulations by appropriate measures. The same applies if service providers are to be used as listed in § 7 section 1, sentence 2.

7.6 Further outsourcing by the subcontractor requires the express consent of the Processor (at the minimum in text form). All contractual provisions in the contract chain shall be communicated to and agreed with each and every additional subcontractor.

## § 8 Supervisory Rights of the Controller

8.1 The Controller has the right, after consultation with the Processor, to carry out inspections or to have them carried out by an auditor to be designated in each individual case. It has the right to satisfy itself of the compliance with this Agreement by the Processor in its business operations by means of random checks, reasonable advance notice of which shall be provided by the Controller.

8.2 The Processor shall ensure that the Controller is able to verify compliance with the obligations of the Processor in accordance with Article 28 GDPR. To this end, the Processor undertakes to make available all information necessary to demonstrate compliance with the obligation laid down in this Agreement upon request of the Controller and, in particular, to demonstrate the execution of the Technical and Organisational Measures.

8.3 Evidence of such measures, which concern not only the specific Order or Contract, may be provided by current auditor's certificates, reports or excerpts from reports provided by independent bodies (e.g. auditor, Data Protection Officer, IT security department, data privacy auditor, quality auditor) or a suitable certification by IT security or data protection auditing (e.g. according to BSI-Grundschutz (IT Baseline Protection certification developed by the German Federal Office for Security in Information Technology (BSI)) or [ISO/IEC 27001](#)).

8.4 The Processor may claim reasonable remuneration for enabling Controller inspections save in such circumstance as the Controller finds that the Processor is not in compliance with this Agreement. Such remuneration shall be calculated according to the usual rates applicable in the sector.

## § 9 Notification of Infringements by the Processor

9.1 The Processor shall assist the Controller in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations, referred to in Articles 32 to 36 of the GDPR. These include:

- a) Ensuring an appropriate level of protection through Technical and Organisational Measures that take into account the circumstances and purposes of the processing as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events.
- b) The obligation to report a personal data breach immediately to the Controller.
- c) The duty to assist the Controller with regard to the Controller's obligation to provide information to the Data Subject concerned and to immediately provide the Controller with all relevant information in this regard.
- d) Supporting the Controller with its data protection impact assessment.
- e) Supporting the Controller with regard to prior consultation of the supervisory authority.

9.2 The Processor may claim compensation for support services which are not included in the description of the services and which are not attributable to failures on the part of the Processor.

## § 10 Controller's Authority to issue instructions

10.1 The Controller shall immediately confirm oral instructions (at the minimum in text form).

10.2 The Processor shall inform the Controller immediately if he considers that an instruction violates Data Protection Regulations. The Processor shall then be entitled to suspend the execution of the relevant instructions until the Controller confirms or changes them.

## § 11 Erasure of Data and Return of personal data

11.1 Upon completion of the contractual work, or sooner, when requested by the Controller, latest upon termination of the Main Agreement, the Processor is obliged to return or destroy (according to data protection requirements following the Controller's approval) all documents, all generated data and usage results arising in conjunction with this Agreement. The same applies to any test data and rejects. The deletion report shall be submitted upon request. Excluded from this regulation are cases where the Parties are obliged to archive the other Party's confidential information due to compelling commercial or tax law provisions as well as if there are reasonable grounds to believe that its destruction could affect the legitimate interests of the affected Party, e.g. for purposes of providing proof of their own legal claims.

11.2 All records demonstrating data processing in compliance with legal obligations are to be kept beyond the term of this Agreement by the Processor. Upon completion of this Agreement, the Processor shall be entitled to return all documentation to the Controller for his discharge.

## § 12 Liability

Art. 82 GDPR shall apply.

Furthermore, the liability provisions of the Main Agreement shall apply.

## § 13 Final Provisions

13.1 Any alterations, modifications, amendments or supplements to this Agreement must be in writing and signed by both Parties. Even a change to the written form requirement requires the written form in order to be valid.

13.2 In the event that any provision of this Agreement or part of it should be or become invalid, the validity of the other provisions of this contract shall not be affected hereby. The invalid provision shall be replaced by a valid provision, which in particular comes closest to the economic intent of the Parties. The same applies in case of a loophole in the Agreement that must be closed.

13.3 This Agreement constitutes the entire agreement between the Parties regarding the subject matter hereof and supersedes any and all prior negotiations, promises, commitments undertakings and agreements of the Parties relating thereto.

13.4 No omission or delay by either Party at any time to enforce any right or remedy reserved to it, or to require performance of any of the terms, covenants or provisions hereof at any time designated, shall be a waiver of any such right or remedy to which either Party is entitled, nor shall it in any way affect the right of either Party to enforce such provisions thereafter.

13.5 Each Party shall bear its own costs in connection with the preparation and execution of this Agreement.

13.6 In the event of any dispute relating to this Agreement, the Parties agree to initially make a full and good faith attempt to resolve such dispute by negotiation at an executive level, to the extent reasonable under the circumstances, prior to commencing court proceedings.

13.7 Should the security of Controller's data be endangered by seizing or confiscating, insolvency or judicial settlement proceedings or any other action taken by third parties, the Processor is obliged to notify the Controller without delay.

13.8 German law shall apply as well as the applicable mandatory EU legislation.

13.9 Place of jurisdiction shall be Kassel, Germany.

## Technical and Organisational Measures

of  
Management Services Helwig Schmitt GmbH  
Garnisonstraße 12  
34369 Hofgeismar  
Germany

As non-public contractor processing sensitive data within the scope of an Agreement for commissioned data processing, we have to take technical and organisational procedures in order to ensure the compliance with the applicable data protection laws. Above all, confidentiality, integrity, availability and resilience of systems and components are to be guaranteed.

Below please read the technical and organisational measures realised within our organisation:

### 1. Confidentiality

#### a) Access Control/Building Security

No unauthorised access to data processing systems, e.g. magnetic- or chip cards, keys, electrical door opener, plant security resp. janitors, alarm systems, video surveillance.

- Alarm system
- Locking system with code lock
- Light barriers / motion sensors
- Key transfer regulation (hand-over of keys etc.)
- Recording visitors
- Commitment of special selected cleaning staff
- Perimeter fencing
- Access control by chip card / transponder
- Video surveillance of exteriors
- Safety locks
- Identity check upon arrival

#### b) Physical Access Control / System Protection

No unauthorised use of the data processing systems, e.g.: (secure) passwords, automatic blocking/locking mechanisms, two-factor authentication, encryption of data carriers.

- Internal access control (permission for user rights)
- Strong password specification
- Authentication with user name/ password
- Locking server housing / computers
- Locking external interfaces (USB etc.)
- Intrusion detection systems
- Encryption of smartphone content
- Encryption of data media on laptop computers
- Use of individual user names
- Biometric authentication
- Assignment of user profiles to IT systems
- Use of VPN technology (remote access)
- Encryption of mobile data media
- Central smartphone administration (e.g. remote deletion)
- Application of software firewall
- Quarantine Network

#### c) Electronic Access Control/Securing Access Authorisation

No-unauthorised reading, copying, changing or deletions of data within the system, e.g. rights authorisation concepts and need-based rights of access, logging of access.

- Rights authorisation concept
- Number of system administrators "reduced to a minimum"
- Logging of system access events, especially entries, changes and deletions of data
- Physical deletion of media prior to reuse
- Secure storage of data carriers
- Encryption of data carriers
- Application of hardware firewall
- Rights management by system administrator
- Password policies, incl. defined password length, password changes
- Use of appropriate shredders resp. specialized service providers (if possible with privacy seal)
- Proper destruction of data carriers (DIN 66399)
- Recording of deletion
- Application of virus protection
- Application of software firewall

#### d) Separation control/Measures to safeguard the separation of purposes for which personal data have been collected

The isolated processing of data, which have been collected for different purposes, e.g. multi-client support, sandboxing, physical or virtual separation of systems.

- Definition of an authorisation concept
- Division between productive and testing systems
- No productive data in testing systems
- Logical client separation (software based)
- Encryption of data records, processed for the same purpose.

## e) Pseudonymisation

The processing of personal data in such a way, that the data cannot be associated with a specific data subject without the assistance of additional information, provided that this additional information is stored separately, and is subject to appropriate technical and organisational measures.

- Pseudonymously (or anonymous) processing of data
- Separation of assignment file and storage in a separate, secure IT system

**2. Integrity**

## a) Data Transfer Control/Data Transfer Security

No unauthorised reading, copying, changes or deletions of data with electronic transfer or physical transport

- Establishment of dedicated lines resp. VPN-tunnel
- Email encryption
- Recording of data recipients as well as periods of scheduled transmission resp. agreed deletion periods
- Physical transport: Selection of special transport staff and carrier
- Encrypted data transfer (e.g. via https or SFTP)
- Data transfer in an anonymous or pseudonymous way
- Creation of an overview of regular data request as well as data transfer
- Physical transport: Use of secure transport containers/-packing
- Use of encrypted external devices when transferring data (CD, USB stick etc.)
- Retention of a filing system to evaluate the origin of data transmitted to automatically processed data

## b) Input Control

Assessment to check and establish whether and by whom personal data have been entered into data processing systems, modified or removed, e.g. logging system, document management

- Use of individually assigned usernames (no user groups) in order to ensure access control of input, modification or deletion of data
- Continual logging of inputs, modification and deletion of data
- Permission settings to entitle to input, modify and delete data in accordance to a right allocation concept
- Retention of a filing system to evaluate the origin of data transmitted to automatically processed data

**3. Availability and Resilience**

## a) Availability control and protection to prevent accidental or wilful destruction or loss

- Uninterruptible power supply (USV)
- Server rooms equipped with monitoring devices for temperature and humidity
- Fire- and smoke detectors
- Server equipped with security fire doors
- Introduction of a back-up and recovery concept
- Server rooms are located beyond the waterline (flood zones only)
- Regular system health monitoring/back-up
- Regular database back-up
- Server rooms equipped with air conditioning
- Server rooms equipped with protective plugs
- Server rooms equipped with fire extinguishers
- Back-ups stored separately in a safe place
- Emergency plan
- No server rooms below sanitary facilities
- Regular data file back-ups

## b) Rapid Recovery

- Recovery acc. to back-up- and recovery concept
- Recovery testing
- Supervision emergency plan

**4. Procedures to handle regular review, valuation and evaluation**

## a) Data Protection Management

- The principles relating to processing of personal data (collection, processing or use) are subject to an internal company policy.
- The data protection officer has been designated in written form.
- The data protection officer is involved in the data protection impact assessment.
- The data protection officer is member of the organizational chart.

- Employees are committed to data confidentiality / handling of personal data.
- Employees are committed to comply with the regulations regarding the secrecy of telecommunications.
- An internal list of processing operations is available.
- Employee training courses.
- Implementation of a control system designed to detect unauthorized access to personal data.

b) Incident Response Management

Incident management in case of detected or suspected security incidents resp. failure related to IT sectors.

- Processing scheme for incident management
- Team practicing realistic exercises
- Security team designated and trained

c) Data protection by implementation of appropriate technical measures and privacy by default settings

- Adherence to privacy by Design/data protection by appropriate technologies
- Selection of privacy-enhancing technologies for future requirements
- Adherence to privacy by Default/data protection by appropriate settings

d) Supervision/Engagement of sub-contractors

No data processing is to be carried out without prior specific authorisation of the Controller, e.g. clear contractual obligation, formalized order management, strict selection of the service provider, obligation for advance verification, follow-up inspection.

- Selection of (sub) contractors subject to professional diligence (in particular with regard to data security)
- Guidelines drawn up for Processor documented in writing (e.g. by data processing Agreement)
- Processor designated data protection officer (if necessary)
- Effective Controller's supervision rights agreed
- Prior to engagement, verification of security measures recorded by sub-contractor
- Processor's employees are committed to sign a secrecy/confidentiality Agreement
- Ensure erasure or destruction of data after termination of the contract
- Continuous review of Processor and his activities

**Status: August 2022**