DATA PROCESSING AGREEMENT

Preamble

THIS DATA PROCESSING AGREEMENT made and entered into this [__] day of [month] [year] (the "Effective Date"), by and between, [Customer], a company having its registered office located at [street address], [Country] (subsequently referred to as "customer"), and AMAGNO GmbH & Co. KG, a company having its registered office located at Bloherfelder Strasse 130, 26129 Oldenburg, Germany/Deutschland (subsequently referred to as "supplier").

Introduction

WITNESSETH WHEREAS the customer commissions the supplier with the provision and maintenance of a software solution, as well as with related services, and support in case of problems. The supplier processes personal data for the customer pursuant to the GDPR Art. 4 No. 2 and Art. 28. This agreement specifies the data protection obligations of the contractual parties resulting from the commission of the supplier. This agreement applies to all activities where the supplier collects, processes and/or uses the customer's personal data.

1. Definitions

In this agreement:

1.1 "Agreement" means this agreement and any amendments to this agreement from time to time;

1.2 "Data processing" or "processing" means any operation or series of operations performed with or without the support of automated procedures related to personal data, such as the collection, organisation, sorting, storage, adaptation, alteration, reading, consultation, use, disclosure by transmission, dissemination or any other form of provision, comparison or linking, restriction, erasure or destruction;

1.3 "Data protection laws" means all applicable laws and corresponding regulations relating to the processing of personal data while they are in force and applicable to personal data, including the General Data Protection Regulation otherwise known as GDPR (Regulation (EU) 2016/679);

1.4 “Effective date” means the date upon which this agreement is signed by both parties and from which this agreement is therefore effective;

1.5 "Instruction" means the arrangement of the contracting authority pursuant to the GDPR Art. 29, directed to a specific purpose by the supplier regarding personal data (e.g. anonymization, blocking, deletion, publication). The instructions are initially defined by this agreement and can be amended, supplemented or replaced by the customer through a single instruction;

1.6 “Main contract” means the contract or agreement entered into between the parties at the point of sale, as it may be amended and updated from time to time;

1.7 "Personal data" means any information related to an identified or identifiable natural person (subsequently referred as "data subject"). An identifiable natural person is one who can be identified, directly or indirectly, by association with an identifier such as a name, an identification number, location data, an online identifier or one or more special features that express the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person.

2. Object of Agreement

2.1 The customer commissions the supplier with the processing of personal data for the exclusive purposes mentioned under article 2.2 of this agreement and to the mentioned extent.

2.2 The object of this agreement is the execution of the following tasks by the supplier:

2.2.1 Contact within the scope of the AMAGNO sales process;

2.2.2 Support and consultancy services for the provided software.

2.3 The agreed service is provided exclusively in a member state of the European Union or in a State Party of the European Economic Area. Any transfer or partial relocation to a third country requires the prior authorisation of the customer and may only take place if the special requirements under article 44 of the GDPR are fulfilled.

2.4 The agreement begins on the effective date and is established for an indefinite period. The agreement can be terminated by the supplier upon observance of the statutory period of cancellation, but not before the end of the main contract. The customer has the right to terminate the agreement at any time without notice in case of a serious breach by the supplier

against data protection laws or against the provisions of this agreement. The agreement can be terminated if the supplier is unable or unwilling to fulfil the customer's request or if the supplier refuses to grant control rights. In particular, failure to comply with the obligations agreed in this agreement and derived under article 28 of the GDPR constitutes a serious breach.

3. Type and Purpose of Processing; Type of Personal Data and Concerned Data Categories

3.1 The scope and purpose of the collection, processing and / or use of personal data (as per article 4 of the GPDR) is as follows:

3.1.1 Establishing contact to verify the data

3.1.2 To generate quotations, order confirmations and invoices

3.1.3 Contact in the framework of consultation, implementation or support for the provided software solution

3.2 The type of personal data (as per article 4 of the GPDR) is as follows:

3.2.1 Basic personal data (first name, surname, address)

3.2.2 Data for communication (e.g. telephone, e-mail, IP address)

3.2.3 Basic contract data (contractual relationship, product or contractual interest)

3.2.4 Customer History

3.2.5 Contract billing and payment data

3.2.6 Planning and control data

3.3 The categories of concerned parties (as per article 4 of the GPDR) are as follows:

3.3.1 Customers

3.3.2 Prospective Buyers

3.3.3 Subscribers

3.3.4 Employees

3.3.5 Suppliers

3.3.6 Sales Representatives

3.3.7 Point of Contact

3.4 Even after the termination of the agreement, the customer can request the handover or deletion of their data, insofar as such data has not already been deleted due to expediency or other legal and / or contractual deadlines. The contents of this agreement shall apply in accordance with it, insofar as the supplier carries out the inspection or maintenance of automated processes or data processing systems covered by the main contract, whereby access to personal data cannot be excluded.

4. Rights and Obligations, including the customer's authority to issue instructions

4.1 The customer is solely responsible for determining the admissibility of the processing and for safeguarding the rights of the data subjects pursuant to the GDPR. Nevertheless, the supplier is committed to immediately forward all these inquiries to the customer, given that they are directed to the customer only.

4.2 Changes to the subject matter of processing and changes to procedures must be agreed jointly between the customer and the supplier and specified either in writing or in a documented electronic format (email is sufficient).

4.3 The customer issues all instructions and partial instructions either in writing or in a documented electronic format (email is sufficient). Verbal instructions must be immediately confirmed in a written form or in a documented electronic format.

4.4 The customer is entitled to obtain adequate evidence of compliance by the supplier regarding the technical and organisational measures taken. Furthermore, the customer is also entitled to ensure compliance with the obligations laid down in this contract before the start of processing and regularly thereafter.

4.5 The customer shall immediately inform the supplier if he detects errors or irregularities in the examination of the order.

4.6 The customer is obliged to treat all supplier business information and data security measures acquired within the scope of the contractual relationship, in a confidential manner. This obligation remains effective even after this contract has ended.

5. Customer and supplier Legal Representatives

5.1 The customer's legal representatives are:

5.1.1 The Managing Director or the Company Board

5.1.2 Those who can identify themselves by means of authorization (e.g. PIN or customer password)

5.1.3 The designated Project Managers

5.2 The supplier's legal representatives are:

5.2.1 The Managing Director or the Company Board

5.2.2 Support Staff

5.2.3 The designated Account Managers and Project Managers

5.3 Communication channels for instructions:

5.3.1 To communicate by email, please use the following address: hello@amagno.co.uk

5.3.2 To contact us by telephone, please call the following number +49 441 309 123 00

5.4 In the event of a change, or if the designated contact person is unable to reply for a long period of time, the other party must be informed immediately, via email or in written form if the successor or the representatives are not available. The instructions must be stored for their period of validity and subsequently for three years.

6. Obligations of the Supplier

6.1 The supplier will process personal data exclusively within the framework of the agreements and in accordance with the customer's instructions, unless the supplier is obliged to do

otherwise under the Member State Law that applies to the supplier (e.g. investigations by law enforcement or state protection authorities). In this case, the supplier shall inform the responsible party of these legal requirements prior to any processing, unless the law in question prohibits such disclosure because of an important public interest, as per Data Protection laws.

6.2 The supplier will not use the personal data provided for any other purposes, especially not for their own benefit. Copies or duplicates of personal data will not be made without the knowledge of the customer.

6.3 After processing personal data in accordance with the contract, the supplier guarantees the execution of all agreed measures. The supplier guarantees that the data processed for the customer will be strictly separated from other databases.

6.4 The databases provided by the customer or used for the customer are marked. Logging in and logging out, as well as the current usage, will be documented.

6.5 In the exercise of the rights of the concerned parties as per Data Protection laws, the supplier will follow the procedure relevant to necessary data protection impact assessments on behalf of the customer. The supplier shall support the customer as far as and must forward the required information to the legal representative of the customer as established in this agreement.

6.6 The supplier will immediately draw the attention of the customer to this, if the supplier considers that an indication given by the customer violates legal regulations, as established in Data Protection laws. The supplier is entitled to suspend the execution of the corresponding instruction until it is confirmed or changed by the responsible party.

6.7 The supplier must correct, delete or restrict the personal data from the contractual agreement if the customer demands to do so by means of instructions, and if this does not oppose the supplier's legitimate interests.

6.8 Information on personal data from the contractual relationship or from the concerned individuals may only be provided to third parties by the supplier after prior instruction or approval by the customer.

6.9 The supplier agrees that the customer is entitled – by appointment - to comply with the regulations on data protection and data security as well as the contractual agreements to an appropriate and necessary extent -by itself or by third parties- commissioned by the customer.

This is achieved by obtaining information and auditing the stored data and its processing, as well as on-site inspection and verification.

6.10 The supplier guarantees that, if necessary, they will assist in the following inspections:

6.10.1 Upon request, the supplier shall provide the customer with suitable evidence of compliance with the obligations pursuant to data protection laws. This evidence can be provided by documents and certificates, which represent approved rules of practice or approved certification procedures pursuant to data protection laws.

6.11 The customer shall grant the supplier (or third parties commissioned by the supplier which require access) the use of data at its premises or at those of the subcontractors. Such access shall be upon request and by appointment. These services are free of charge. The data may only be processed in private locations (telework or the employee's home) with the consent of the customer. If the data is processed in a private home, access must first be contractually guaranteed for the employer's control purposes.

6.12 The supplier confirms that the customer is aware of the relevant data protection laws, which are relevant execution of any contractual agreements. The supplier will also assure that, prior to work, the supplier will acquaint the personnel employed in carrying out the work with the data protection provisions applicable to them and will undertake to maintain appropriate confidentiality for the duration of their work and after termination of the work relationship as per data protection laws. The supplier shall monitor compliance with data protection laws within the supplier's company.

6.13 For data protection issues the customer can contact the supplier via the following email address: privacy@amagno.co.uk

7. Obligations of the Supplier to Notify in the Event of Processing Disruptions and Violations of Personal Data Protection

7.1 The supplier shall notify the customer immediately about the removal or modification of any approved regulation code, as well as the revocation of any relevant certification, pursuant to data protection laws. The supplier shall immediately notify the customer of any disruptions or infringements made by the supplier or its employees. The supplier shall also report infringements of relevant data protection clauses or agreement stipulations as well as the suspicion of data protection violations or irregularities in personal data protection. This applies to any reporting and notification obligations of the supplier pursuant to data protection laws. The supplier guarantees to support the customer reasonably, according to

its obligations under data protection laws. Notifications to the customer may only be made by the supplier if it fulfills the stipulations established in this agreement.

8. Subcontractual Relationship with Subcontractors

8.1 The supplier is only allowed to commission subcontractors to process the customer's data with the permission of the relevant party, which must be carried out via one of the communication channels established in this agreement, in accordance with instructions given by the customer. Consent may only be given if the supplier informs the customer the name and address as well as the intended activity of the subcontractor. Furthermore, the supplier must ensure that the subcontractor is carefully selected, taking into account the suitability of the technical and organisational measures taken by the subcontractor as per data protection laws. The relevant documentation must be made available to the customer upon request.

8.2 Subcontracting in non-EU countries may only take place if the special requirements of data protection laws are fulfilled (e.g. Commission adequacy decision, standard data protection clauses, approved codes of conduct).

8.3 The supplier must ensure that the agreed regulations between the customer and the supplier also apply to subcontractors. The contract with the subcontractor shall specify the details in such detail that the responsibilities of the supplier and the subcontractor are clearly defined. If several subcontractors are involved, this shall also apply to the responsibilities between these subcontractors. The customer must be entitled, if necessary, to carry out appropriate inspections (including on-site inspections) amongst subcontractors or by third parties assigned by the customer.

8.4 The contract with the subcontractor must be concluded either in written or in electronic format.

8.5 Forwarding data to the subcontractor is only allowed if the subcontractor has fulfilled the obligations regarding its employees.

8.6 The supplier shall verify that the obligations of the subcontractor(s) are fulfilled in accordance with the arrangements made between the supplier and the customer under the present agreement.

8.7 The result of the inspections shall be documented and made available to the customer upon request.

8.8 The contractor shall be responsible for guaranteeing that the subcontractor complies with the data protection obligations imposed by the supplier in accordance with this section of this agreement.

8.9 The subcontractors specified in Appendix 2 with name, address and order content are currently engaged in the processing of personal data to the extent specified there for the supplier. The customer hereby agrees to the commissioning of said subcontractors.

8.10 The supplier will inform the person in charge of any intended change in relation to the use of new subcontractors or the replacement of existing subcontractors, giving the customer the possibility to object to such changes.

9. Technical and Organisational Measures

9.1 A level of protection appropriate to the risk of rights and freedoms concerning the natural persons, shall be guaranteed for the specific processing of the contract. In this context, the protection objectives of data protection laws, such as confidentiality, integrity and availability of systems and services and their resilience regarding the type, scope, circumstances and purpose of processing are considered in such a way that the risk is permanently controlled by appropriate technical and organisational corrective measures.

9.2 The data protection concept described in Appendix 1, describes in detail the selection of technical and organisational measures appropriate to the established risk, considering the protection goals in accordance with the state of the technology and the IT systems and processing methods used by the supplier.

9.3 Data processing standards are ensured by a periodic assessment, evaluation and review of the effectiveness of technical and organisational measures. The supplier shall provide to the customer relevant documentation on request.

9.4 The supplier will carry out a revision, assessment and evaluation of the effectiveness of the technical and organisational measures to guarantee the security of the processing.

9.5 Decisions on data processing and the applied methods, which are important for security, must be agreed between the supplier and the customer.

9.6 If the measures taken by the supplier don't meet the requirements of the customer, the supplier will inform the customer immediately.

9.7 The measures by the supplier taken during the period of the main contract, may be adapted to technical and organisational enhancements, but may not fall below the agreed standards.

10. Obligations of the Supplier After Termination of the Contract

10.1 Upon termination of the main contract, the supplier must hand over all data to the customer. The supplier must delete or destroy said data in accordance with data protection laws, including the documents and generated data or usage results, connected to the relationship established by the main contract.

10.2 The deletion of data must be notified to the customer in a writing or electronic format, including the date of said deletion.

11. Liability

11.1 The supplier is liable for infringements made by the supplier or its subcontractors, regardless of whether the customer has agreed to the intervention or not, pursuant article 82 of the GDPR.

12. Concluding Clauses

12.1 Agreements on technical and organisational measures, as well as controlling and testing documents (also on subcontractors) must be kept by both contracting parties for its validity period (three full calendar years).

12.2 The supplier must inform the customer immediately in case that the data is compromised by a seizure or confiscation, by insolvency or composition proceedings or by third party actions. The supplier shall immediately inform all involved parties that the responsibility for the customer data lies with the customer.

12.3 No collateral agreements to this contract have been made. Modifications and amendments to this contract, unless otherwise instructed, must be made in writing or in electronic format to be legally effective. This also applies to the cancellation of this contract or changes in the procedural requirement.

12.4 If any clause of this contract is completely or partially invalid, or loses its legal validity, the validity of the remaining clauses shall not be affected. In case of an ineffective regulation -

insofar it is legally permissible - another appropriate regulation shall apply, in accordance with the initial wishes and intentions of the parties as established by this agreement. The same shall apply if the contract contains a gap; this gap shall be resolved by a regulation corresponding to the initial wishes and intentions of the parties as established by this agreement.

12.5 This agreement shall be governed by and construed in accordance with the law of the Federal Republic of Germany.

12.6 The courts of Oldenburg in Lower Saxony, Federal Republic of Germany, shall have exclusive jurisdiction to adjudicate any dispute arising under or in connection with this agreement.

12.7 By signing this agreement, the parties acknowledge that they have sufficiently informed themselves about the rights and obligations in accordance with data protection laws, before signing the agreement and that the parties agree to the above.

12.8 The following attachments which are necessary for the signing of this agreement are also enclosed with the agreement:

12.8.1 Appendix 1 - Technical and Organisational Measures Pursuant to article 32 of the GDPR.

12.8.2 Appendix 2 - Subcontractors

APPENDIX 1: Technical and Organisational Measures

This appendix concerns the technical and organisational measures pursuant to Article 32 of the GDPR. If it is relevant, references to the documents/certificates may be provided (as per this Appendix). The internal organisation must be designed in such a way that it meets the special requirements of data protection. This includes:

1. With regard to access control to sites and devices where data is processed, the supplier must ensure the following measures are in place and maintained:

    a. Relevant technical and organisational measures: (in accordance with the state of technology for access control, and for the legitimation of authorised parties).

    b. Key handling is controlled and appropriately documented. There is a log for each key transfer. Central and non-allocated keys are kept safe.

    c. The entrance to the building and offices are permanently closed. Entrance areas and windows are tightly closed outside business hours.

    d. During business hours reception is open and additionally used as access control.

    e. The entrance door can only be opened from the outside with a key or by the reception desk.

    f. All accesses are guarded outside business hours by a monitoring system (alarm system).

    g. Visitors, guests and training participants can only move freely in the training area. Access to the offices is only permitted when accompanied by AMAGNO personnel. Visitors, guests and training participants are not allowed to access the data centre.

    h. The server is located in a closed room which only the administrators have access to.

    i. The data centre is located outside the building. Access is only allowed to a certain group of people. Every entrance and exit is logged.

2. With regard to access control to relevant I.T. hardware, software, accounts and systems, the supplier must ensure the following measures are in place and maintained:

    a. Technical and organizational measures regarding user identification and authentication (password / password protection)

b. Every employee has a personalized account to log on to his or her personal account.

c. All systems are always updated to ensure the best security possible.

d. The access to the systems is individually configured.

e. The number of administrators is limited to the minimum.

f. Automatic lock (e.g. password or timeout/screen lock)

g. AMAGNO's network is protected against external access by a virus protection firewall

h. Remote maintenance access to the servers and external access from terminal devices outside the network are secured via a VPN connection.

i. Only temporary passwords are assigned, which the user must change. The passwords cannot be seen by the administrator.

j. Design of the authorization and access rights, as well as monitoring and logging.

k. Access to notebooks, desktops and servers is only through personalised authentication. The permissions are set up according to the "need to know" principle (profiles, roles, transactions and objects e.g.: limit access to folders).

l. AMAGNO uses appropriate password rules such as special characters, minimum length and regular password changes.

m. Access is blocked after a certain number of failed attempts.

n. Former employees' accounts are deactivated immediately after leaving the company.

o. Data that is no longer required is properly deleted.

p. AMAGNO does not operate "shared accounts", e.g. where more than one person has access to the account.

3. With regard to data transmission protocols, the supplier must ensure the following measures are in place and maintained:

a. Personal data transmission (electronic transmission, data transmission, control of transmission, etc.) must be regulated to prevent loss, alteration or unauthorised publication.

b. Measures during the transportation, transmission and data storage (manual or electronic) as well as during subsequent inspections:

c. Personal data is transmitted online via VPN connection or SSL/TLS encrypted connection.

d. In justified and exceptional cases, data can be sent in a password-protected file or encrypted e-mail after prior consultation and approval by the customer. The file' s password is communicated to the receiver through another path.

e. Personal data will not be transferred to external data storage devices.

f. An agreement concerning the contract processing is concluded with all the concerning parties.

g. All employees who handle personal data are under a written confidentiality agreement.

Personal data processing is carried out in such a way that the data can no longer be assigned to the concerned party without the use of additional information, and this additional information is kept separately and corresponds to technical and organisational measures as per data protection laws and specifically the GDPR. Personal data originates from the applications used by AMAGNO and these are indispensable in the context of processing. If the personal data is pseudonymised, it would lead to unacceptable obstacles to its adequate processing. Therefore, pseudonymization in these applications would not be admissible.

4. With regard to Input Control, the supplier must ensure the following measures are in place and maintained:

a. Traceability and documentation of data management and maintenance must be guaranteed.

b. Measures for subsequent verification, and by whom data have been entered, changed or removed (deleted):

c. In the systems used by AMAGNO, where personal data is processed, it is possible to check at any time when and by whom personal data were entered, changed or deleted. This can also be checked afterwards, because all changes are logged.

d. All documents are stored in a document management system compliant to the GDPR and GOBD (German Finance Ministry Business Accounting Regulations).

5. With regard to monitoring of instructions, the supplier must ensure the following measures are in place and maintained:

    a. It is the responsibility of AMAGNO's management to ensure that personal data is only processed in the business workflows in accordance with the instructions of the customer and in accordance with the applicable legal regulations.

    b. There are clear rules concerning competences and responsibilities.

    c. All distributors and subcontractors are carefully selected.

    d. After termination of the contractual relationship, all data no longer required will be deleted.

6. With regard to Security and Availability of data, the supplier must ensure the following measures are in place and maintained:

    a. Data must be protected against accidental destruction or loss.

    b. All data is regularly backed up online according to a data backup procedure to ensure the greatest availability.

    c. The integrity of the I.T. systems is ensured by appropriate measures.

    d. Uninterruptible power supplies (UPS) are used to prevent data loss due to a power failure.

    e. All servers are protected against attacks by appropriate measures (virus protection / firewall).

7. With regard to Independency of Control, the supplier must ensure the following measures are in place and maintained:

    a. Data collected for different purposes shall also be processed separately.

    b. Measures for the separate data procedure used for different purposes (storage, modification, deletion, transmission):

    c. The different applications are separate from each other. Management within the systems ensures that only authorized users have access.

d. Separation of functions (production / test)

e. Logical separation of data

8. With regard to Procedures for regular review, assessment and evaluation, the supplier must ensure the following measures are in place and maintained:

   a. Data protection is the responsibility of the entire company.

   b. I.T. security must be kept up-to-date.

   c. Data protection-friendly technologies are used when possible and economically viable.

   d. Regular awareness campaigns and employee training.

   e. Definition of responsibilities.

   f. Customer instructions within the scope of order processing are documented on a customer-oriented basis.

   g. Activities performed in the context of order processing are documented on a customer-oriented basis.

9. With regard to incident response, the supplier must ensure the following measures are in place and maintained:

   a. There are internal processes and instructions for data protection, which can be extended or supplemented if necessary.

10. With regard to Data protection friendly-presettings. the supplier must ensure the following measures are in place and maintained:

    a. In the implemented systems, the highest protection level is always used when creating new users. New users have no rights in the systems. These are not assigned until the role is assigned.

END OF APPENDIX 1

APPENDIX 2: Subcontractors

Supply as established in the main contract, in addition to other partial services, are carried out with the assistance of subcontractors who are involved in this project.

Please check the following options accordingly:

- ☑ Subcontractors will NOT be used.
- ☐ Only subcontractors from Germany will be used.
- ☐ Subcontractors from EU/EEA area will (also) be used.
- ☐ Subcontractors from non-EU countries outside the EEA (European Economic Area) will (also) be used.

The following is the list of all subcontractors who are directly involved in the provision of services for the customer and who may or could have access to the customer's data. This also includes external I.T. service providers with corresponding access rights. As a rule, this does not include telecommunications services or postal/transport services.

Subcontractor Company, location and point of contact	Description of the Service (Activities of the subcontractor)
1.	
2.	
3.	
4.	
5.	

END OF APPENDIX 2