Data Processing Agreement

The Processor,

rocon Rohrbach EDV-Consulting GmbH

Isaac-Fulda-Allee 1

55124 Mainz

Germany

processes personal data on behalf of the Controller (together the “Parties”), as defined by Article 28 of the EU General Data Protection Regulation (GDPR). This Data Processing Agreement (hereinafter “DPA”) applies to all contractual relationships between the Parties, which refer to this DPA. The Controller is rocon’s Customer, as defined in the respective Individual Contract(s) (hereinafter “Main Contract”) between the Parties. The details of the contractual agreements between the Parties are set out in the Main Contract for the respective Products and/or Services.

For this processing on behalf of the Controller, the Parties agree as follows:

§ 1 Subject Matter of the DPA

(1) The Processor will process personal data on behalf of the Controller. Subject matter, nature and purpose of the processing of personal data by the Processor for the Controller are specified in Main Contract as well as in the statement of work referred to in the Main Contract.

(2) The Data Subjects covered by the assignment and the associated rights of access to their data are listed in Appendix 2.

(3) The duration of this DPA is the same as the duration of the Main Contract and the respective statement of work (see also Appendix 1). The obligation to observe data secrecy and confidentiality will continue even after this DPA is terminated.

(4) Changes to the subject matter of processing, scope of processing as well as changes of procedures must be agreed in writing.

(5) The processing and use of the data takes place exclusively in the territory of Germany, in a Member State of the European Union or another State that is Party to the Treaty on the European Economic Area (EEA). Every transfer of personal data to a third country outside of the EEA must be approved by the Controller prior to the transfer and can only take place if the special requirements from Articles 44 to 49 GDPR are met.

§ 2 Processor's Obligations

(1) The Processor will perform the Products and/or Services exclusively in accordance with the DPA and as instructed by the Controller. The Processor is obliged to document instructions from the Controller immediately. The Processor has to inform the Controller immediately, if the Processor believes that an instruction violates applicable law.

(2) The Processor processes personal data that it has received as part of the fulfilment of this DPA solely for the agreed contractual purposes. The Processor is prohibited from processing or using

such personal data without the knowledge of the Controller or for the Processor's own purposes. The Processor shall make no copies or duplicates without the knowledge of the Controller. This does not include backup copies, as far as these are required to ensure data processing in accordance with the GDPR and this DPA, as well as data required to comply with statutory retention obligations.

(3) The Processor ensures in its area of responsibility, the implementation of and compliance with the agreed technical and organizational measures in accordance with Article 32 GDPR. The concrete requirements are defined in Appendix 3. Both Parties agree that the technical and organizational security measures listed in Appendix 3 are sufficient for the specific risk of the processing according to this DPA. The Processor may change the agreed technical and organizational measures, provided that this ensures at least the same level of security for the personal data of the Controller.

(4) The Processor has designated a Data Protection Officer (DPO) which is named in Appendix 4. The current DPO is listed in the data privacy notice on the Processor's website (https://www.rocon.info/datenschutz).

(5) The Processor will also support the Controller with appropriate technical and organizational measures when responding to requests from Data Subjects in regards to their rights according to Articles 12 to 22 GDPR if legally and de facto feasible. This concerns in particular the right of access by the Data Subject (Article 15 GDPR), the right to rectification (Article 16 GDPR), the right to erasure of personal data (Article 17 GDPR) as well as the right to restriction of processing (Article 18 GDPR). The Processor may only rectify, erase or restrict processing upon documented instructions of the Controller. The Processor shall provide no information concerning personal data to Third Parties, not even to the Data Subjects themselves. As far as a Data Subject makes a request to the Processor, the Processor will forward the request to the Controller without undue delay. To the extent that costs are incurred on the part of the Processor in providing the necessary assistance, the Controller shall reimburse such costs on the basis of the Processor's normal daily/hourly rates, unless the action is required as a result of a violation of this DPA or applicable law for which the Processor is responsible.

(6) The Processor ensures that authorized persons who process personal data have agreed in writing to maintain confidentiality or are subject to an appropriate legal obligation of secrecy.

(7) The Processor will immediately notify the Controller in the event of severe disruptions to its operations, suspected breaches of data protection or any other irregularities in the processing of the Controller's personal data as well as in cases involving violations of the provisions of this DPA. The Processor also informs the Controller immediately about control activities and measures of the supervisory authority and other official bodies that affect the processing of personal data under the scope of this DPA.

(8) Additionally, the Processor supports the Controller, taking into account the nature of the processing and the information available to the Processor, with regards to the Controller's obligations according to Article 33 GDPR (Notification of a personal data breach to the supervisory authority) as well as according to Article 34 GDPR (Communication of a personal data breach to the Data Subject). The Processor also supports the Controller, taking into account the nature of the processing and the information available to the Processor, in conducting the data protection impact assessment, a potentially required consultation with the supervisory authority (Articles 35 and 36 GDPR) as well as other enquiries and controls by official bodies.

Insofar as costs are incurred on the part of the Processor in providing the necessary support, the Controller shall reimburse these costs on the basis of the Processor's usual daily/hourly rates, unless the activities are to be taken as a result of a violation of this DPA or of applicable law for which the Processor is responsible.

(9) The Processor shall maintain a record of all categories of processing activities on behalf of the Controller that complies with the requirements of Article 30 paragraph 2 GDPR. With regards to the record of processing activities of the Controller, the Processor supports the Controller on the Controller's request to the extent feasible.

(10) The Processor provides the Controller upon request with all reasonable information to prove compliance with this DPA. The Processor provides all information reasonably needed to carry out a comprehensive check on written request within a reasonable time.

(11) Data storage devices given to the Processor and any copies or reproductions made thereof remain the property of the Controller. The Processor is required to keep them stored in a safe place in a way that they are not accessible to Third Parties.

§ 3 Controller's Obligations

(1) The Controller is responsible for compliance with applicable data protection laws and protecting the rights of the Data Subjects. Data Subjects' rights are to be asserted against the Controller.

(2) The Controller must immediately and fully inform the Processor if a review of the results of processing reveals errors or irregularities pertaining to data protection regulations.

§ 4 Controller's Rights / Audits

(1) The Controller has the right to issue instructions on the nature, the scope of the data processing as well as the procedure used to process data. The same applies to the specification and updating or upgrading of data security measures. Insofar as these instructions significantly change the obligations of the Processor in the contractual relationship or incur additional costs, they shall be considered as a request for a change of the Main Contract.

(2) The Controller or a representative of the Controller may audit the Processor's operational facilities to ensure appropriate measures are being taken to meet applicable legal technical and organizational requirements of data protection relevant to the processing of Controller's personal data. Such audits may take place only after advance notification, during normal business hours and without interrupting the Processor's operations. The Processor is required to allow such audits and assists the Controller in conducting them. To the extent that the auditor may also see data of other customers of the Processor during the audit, the auditor shall upon request of the Processor sign a non-disclosure agreement prior to an audit.

(3) Upon written request by the Controller, the Processor undertakes to give the Controller within a reasonable time all information reasonably necessary to perform comprehensive data processing audits.

(4) Insofar as costs are incurred on the part of the Processor for the support of audits, the Controller shall reimburse these costs on the basis of the Processor's usual daily/hourly rates, unless the audits have become necessary due to a violation of this DPA or of applicable law for which the

Processor is responsible, or the audit uncovers violations of this DPA or of applicable law by the Processor.

§ 5 Sub-processors

(1) The Processor may outsource tasks to Sub-processors only with written permission from the Controller. This rule and the following rules also apply to Sub-processors.

(2) The Processor has to inform the Controller about every proposed change with regard to new Sub-processors or replacing an existing Sub-processor. The Controller has the right to object to such changes.

(3) The Processor must select each Sub-processor carefully. Before the Sub-processor begins processing personal data and regularly thereafter, the Processor is obliged to check that the Sub-processor has implemented appropriate technical and organizational measures. The results of the examination must be documented. The Controller must be provided with this report upon request.

(4) Whenever the Processor engages Sub-processors, the contractual provisions must be issued in writing and need to be designed in such a way, so that they correspond to the requirements of this DPA, whereby in particular sufficient guarantees have to be in place that the appropriate technical and organizational measures are implemented in such a way that they comply with the requirements of the GDPR and this DPA.

(5) The Controller is entitled to receive, upon written request, from the Processor information about the key contract terms and the fulfilment of obligations pertaining to data protection that is conducted by the Sub-processor. If necessary, such information may also be obtained by inspecting the relevant contract documents.

(6) If the Sub-processor is based in a country other than a Member State of the European Union or the EEA or data processing takes place in such a country, it is also the obligation of the Processor to ensure that the requirements of Articles 44 to 49 GDPR are fulfilled. This must be demonstrated to the Controller in writing before the Sub-processor commences data processing activities.

(7) Authorization to engage the Service Providers named in Appendix 5 is granted if the above requirements are met.

(8) If the Sub-processor fails to comply with data protection obligations, the Processor is liable to the Controller for compliance with the obligations of each Sub-processor.

§ 6 Confidentiality

(1) The Parties undertake to treat any and all information and documents to which they become privy under the scope of this DPA as strictly confidential. This rule applies in particular to business and trade secrets of the respective contracting party. The purpose and content of this DPA must also be treated as confidential. The Parties are obliged to process and use the information and data of the contracting party provided or become known within the scope of the DPA exclusively for the purpose of the DPA. Each Party may process or use data and information for their own purposes and share it with Third Parties only with the prior written consent of the contracting

party, unless the Third Party is a (legal) advisor of the Party with professional confidentiality obligations.

(2) If it becomes necessary to engage Third Parties for the execution of the tasks, it must be ensured that these Third Parties also strictly comply with the signed data protection and non-disclosure agreements. The engagement of Third Parties requires the express consent of the contracting party.

(3) The above rights and obligations shall extend beyond the term of this DPA.

§ 7 Termination of the DPA

(1) Upon termination of the DPA or earlier upon request of the Controller, the Processor shall physically delete or return to the Controller without exception all documents, data storage devices or other results of the data processing at the request of the Controller. The Processor must also declare that neither it nor its Sub-processors possesses any additional copies. Any and all personal data stored by the Processor must be deleted, except for restricted personal data in back-ups, which are deleted after the regular deletion periods. The deletion must be documented. Test and reject materials are to be destroyed or deleted immediately.

(2) Documentation that complies with contract and regular data processing is to be stored according to current retention periods also after the assignment is terminated. For the purpose of discharge, the Processor can transfer this documentation to the Controller after the termination of the contract.

(3) The Controller is entitled to verify compliance with the above obligations, if necessary also on site according to § 4.

§ 8 Miscellaneous and General Provisions

(1) The Processor must inform the Controller without undue delay if the data of to the Controller, which are in possession of the Processor, are threatened with seizure or confiscation, by insolvency or settlement proceedings or any other events or measures taken by Third Parties. In this case, the Processor will without undue delay notify all officials in this context that the Controller maintains sovereignty of the data.

(2) This DPA replaces all previous agreements concerning data protection between the Controller and the Processor.

(3) Changes and amendments to this DPA and all its parts – including any promises made by the Processor – require written agreement and an express notice that the terms of this DPA have been changed or amended. This also applies to a waiver of this written form requirement.

(4) Should individual provisions of this DPA be or become invalid, or if any provisions have been omitted from this DPA, the legal validity of the remaining provisions shall not be affected. In place of the invalid or missing provision, an effective provision, which comes closest to the economic intention of the parties, shall be deemed to have been agreed.

(5) This DPA is governed by German law.

Appendix 1: Specification of Products and/or Services

The activities of the Processor for the Controller within the scope of the processing of personal data of the Controller are to be taken from the statement of work of the Products and/or Services commissioned in each case and the descriptions of the Products and/or Services in the Main Contract.

Insofar as the MIS1001 and MIS1002 Products and/or Services have been commissioned, the processing activity shall also include the hosting of personal data.

No processing of personal data relevant to the DPA is contained in the following products of the Processor:

- CWS1001, CWS1002, CWS1003, CWS1004, CWS 1005,
- CIP2001, CIP2016, CIP2017, CIP2008, CIP2018, CIP2010, CIP2101, CIP2013, CIP2014,
- CTR1001, CTR1002, CTR1003, CTR1004, CTR1005, CTR1006, CTR1007,
- MIS1020, MIS1021, MIS1016, MIS1019,
- A1117,
- SBC003

Appendix 2: Data Subjects and Categories of Data

In accordance with the DPA, the Processor also processes personal data for the Controller. The types of data are specified below. Due to technical advancement and organizational changes, it is possible that the composition of data changes as well.

Data subjects are in particular:

- Current and former employees of the Controller,
- Applicants of the Controller,
- Business and private customers of the Controller (including interested parties) and employees of business customers of the Controller,
- Suppliers of the Controller and employees of suppliers of the Controller,
- Other business partners of the Controller and employees of other business partners of the Controller.

The categories of processed personal data are in particular:

- Master data and communication data (including name, maiden name, title, gender, date of birth, marital status, nationality, language),
- Identity data (including personnel number),
- Private and professional contact data (including address, e-mail address, telephone number, mobile number),
- Application documents (qualifications, education, references, etc.),
- Travel request data (including travel activity, travel costs, travel destination, reason for travel, travel expenses),
- Organizational assignment of employees (including department affiliation, cost center, job description, employee group, position in the company),
- Wage and salary data and credit card data,
- Time recording data,
- Employee data in CRM systems (sales, service center),
- Incident management/ticket systems,
- IT system-specific data, such as user name, access rights, user profiles.

No special categories of personal data according to Art. 9 GDPR will be processed.

Appendix 3: Technical and Organizational Security Measures

Overview on the implemented Technical and Organizational Measures

1. Physical Access Control

Technical Measures	Organizational Measures
☐ Alarm system	☒ Key policy / Concept
☒ automatic physical access control	☒ reception / gatekeeper
☐ biometric access control	☒ visitor book / protocol of visitors
☒ chip cards / transponder systems	☒ employee - / visitor badges
☐ Manual locking system	☒ Visitors accompanied by employees
☒ security lock	☒ careful selection of security services
☐ Locking system with code lock	☒ careful selection of cleaning services
☒ Protection of building shafts	☐
☒ Doors with knob outside	☐
☒ Doorbell system with camera	☐
☐ Video surveillance of entrances	☐
☒ Measures against the effects of natural disasters, intentional attacks or accidents	☐
☐	☐

2. Logical Access Control

Technical Measures	Organizational Measures
☒ Login with username + password	☒ management of user rights
☐ Login with biometric data	☒ Creating user profiles
☒ Anti-virus software server	☒ Central password assignment
☒ Anti-virus software clients	☒ password policy
☐ Anti-virus software mobile devices	☒ Delete / Destroy" policy
☒ Firewall	☒ Clean desk policy
☒ Intrusion Detection System	☒ General policy data protection and / or security
☐ Mobile Device Management	☒ Mobile Device Policy
☒ Encryption of data carriers	☒ Manual desktop lock" guide
☒ Encryption of smartphones	☐
☐ Case lock	☐
☐ BIOS protection (separate password)	☐
☒ Locking of external interfaces (USB)	☐
☒ Automatic desktop lock	☐
☒ Laptop/tablet encryption	☐
☐	☐

3. Access Control

Technical Measures	Organizational Measures
☒ Document shredder (min. level 3, cross cut)	☒ Use of authorization concepts
☒ External document shredder (DIN 32757)	☒ Minimum number of administrators
☐ Physical deletion of data carriers	☒ Data vault
☒ Logging of accesses to applications, specifically when entering, changing, and deleting data	☒ Management of user rights by administrators
☒ Rules for encryption to protect information during storage and transportation	☒ "Delete / Destroy" policy
☐	☐

4. Separation Control

Technical Measures	Organizational Measures
☒ Separation of productive and test environment	☒ Control via authorization concept
☐ Physical separation (systems / databases / data carriers)	☒ Definition of database rights
☒ Multi-client capability of relevant applications	☐ Data records are provided with purpose attributes
☐	☐

5. Pseudonymization

Technical Measures	Organizational Measures
☒ In the case of pseudonymization: separation of the assignment data and storage in separate systems (possibly encrypted).	☐ Internal instruction to anonymize / pseudonymize information as far as possible in the event of disclosure or even after the expiry of the statutory deletion period.
☐	☐

6. Transfer Control

Technical Measures	Organizational Measures
☒ E-mail encryption	☐ Documentation of the data recipients and the duration of the planned transfer or deletion periods.
☒ Use of VPN	☐ Overview of regular retrieval and transmission processes
☐ Logging of accesses and retrievals	☐ Transfer in anonymized or pseudonymized form
☐ Secure transport containers	☒ Care in the selection of transport personnel and vehicles
☒ Provision via encrypted connections such as sftps, https	☐ Personal handover with protocol
☐ Data transfer via OFTP2	☐
☐ Use of signature procedures	☐
☐	☐

7. Input Control

Technical Measures	Organizational Measures
☒ Technical logging of the entry, modification, and deletion of data.	☒ Overview of which programs can be used to enter, change, or delete which data.
☐ Manual or automated control of logs	☒ Traceability of data entry, modification, and deletion by individual user names (not user groups)
☐	☒ Assignment of rights for entering, changing, and deleting data on the basis of an authorization concept.
☐	☐ Retention of forms from which data has been transferred in automated processing
☐	☐ Clear responsibility of deletions
☐	☐

8. Availability Control

Technical Measures	Organizational Measures
☒ Fire and smoke detection system	☒ Back-up & recovery concept
☒ Fire extinguisher server room	☒ monitoring of the backup process
☒ Server room air-conditioned	☒ Regular data recovery tests and logging of results
☒ UPS (uninterruptible power supply)	☒ Storage of backup media in a secure location outside the server room
☒ Protective socket strips server room	☒ No sanitary connections in or above the server room
☐ Data safe	☐ Existence of an emergency plan/ BCM
☒ RAID system / hard disk mirroring	☒ Separate partitions for operating systems and data
☒ Video surveillance server room	☐
☒ Alarm message in case of unauthorized access to server room	☐
☒ Use of VMware high availability solution	☐
☒ Use of Veeam Backup & Replication technology	☐
☒ Proactive Care for storage systems	☐
☐	☐

9. Data Protection Management

Technical Measures	Organizational Measures
☐ Software solution for data protection management in use	☒ External data protection officer **Dr. Jörn Voßbein /** **UIMC Dr. Voßbein GmbH & Co KG /** **datenschutz.rocon@uimc.de** **0202 9467726200**
☒ Central documentation of all procedures and regulations for data protection with access for employees as required / authorized (via Wiki; Intranet ...)	☒ Employees trained and obligated to confidentiality / data secrecy
☐ Security certification according to ISO 27001, BSI IT-Grundschutz, or ISIS12	☒ Regular training of employees (annually)
☒ Other documented security concept	☐ Internal / external information security officer **Name / Company / Contact details**
☒ A review of the effectiveness of the technical protective measures is carried out at least annually	☒ Data protection impact assessment (DSFA) is carried out as required
☐	☒ The organization complies with the information obligations under Articles 13 and 14 of the GDPR
☐	☒ Formalized process for handling requests for information from data subjects is in place
☐	☒ Confidentiality agreements are concluded before information is exchanged, and the requirements or needs for protecting information are documented and regularly reviewed
☐	☐

10. Incident Response Management

Technical Measures	Organizational Measures
☒ Use of firewall and regular updating	☒ Documented process for detecting and reporting security incidents/data breaches (also with regard to the obligation to report to authorities)
☒ Use of spam filter and regular updating	☒ Documented procedure for dealing with security incidents
☒ Use of virus scanner and regular updating	☒ Involvement of DPO in security incidents and data breaches
☒ Intrusion Detection System (IDS)	☒ Documentation of security incidents and data breaches, e.g., via ticket system
☒ Intrusion Prevention System (IPS)	☒ Formal process and responsibilities for the follow-up of security incidents and data breaches
☒ Information about technical vulnerabilities of the IT systems is obtained promptly, assessed, and appropriate measures are taken	☐
☐	☐

11. Privacy by Default

Technical Measures	Organizational Measures
☒ No more data is collected than is necessary for the respective purpose	☐
☐ Simple implementation of the revocation of a data subject by technical measures	☐
☐	☐

12. Data Processing Supervision (in case sub processors are being used)

Technical Measures	Organizational Measures
	☒ Prior review of the safety measures taken by the contractor and their documentation.
	☒ Careful selection of the contractor
	☒ Conclusion of the necessary agreements on commissioned processing and/or EU standard contractual clauses
	☒ Written instructions to the contractor
	☒ Obligation of the contractor's employees to maintain information secrecy
	☐ Obligation for the contractor to appoint a data protection officer
	☐ Obligation for the contractor to appoint an information security officer
	☒ Agreement on effective control rights vis-à-vis the contractor
	☒ Ensuring the destruction of information after termination of the contract
	☒ In case of longer cooperation: Ongoing review of the contractor and its level of protection
	☒ Confidentiality agreements are concluded before information is exchanged, and the requirement or requirements for protecting the information are documented and regularly reviewed
	☐

Appendix 4: Data Protection Officer

Processor's Data Protection Officer:

Name:	Dr. Jörn Voßbein (UIMC Dr. Voßbein GmbH & Co KG)
Address:	Otto-Hausmann-Ring 113, D-42115 Wuppertal
Phone number:	(0202) 265 74 - 0

Appendix 5: Sub-processors according to Section 5 of the Data Processing Agreement

As far as the products MIS1001 and MIS1002 have been ordered, the Processor uses the following service providers in the context of hosting the data in the rocon cloud:

Name of company:	NetPlans GmbH
Address:	Eisenstockstraße 12, 76275 Ettlingen, Germany
Type of service:	Hosting of the Controller's personal data within MISTRAL. The data is operated in a TelemaxX data center in Karlsruhe (Germany). The operation of the data center is certified in accordance with DIN ISO 27001, DIN ISO 27017 and DIN ISO 27018. The Processor will provide the data processing contract with NetPlans upon request.
DPO contact information:	datenschutz@netplans.de

Name of company:	STACKIT GmbH & Co. KG
Address:	Stiftsbergstraße 1, 74172 Neckarsulm, Germany
Type of service:	Data center services and operations.
DPO contact information:	datenschutz@mail.schwarz