Data Processing Agreement

This Data Processing Agreement regulates data processing on behalf of the Client by cioplenu GmbH, Am Technologiezentrum 5, 86159 Augsburg, Germany, as a Contractor. It is part of the Main Contract on the provision of the Operations 1 Software to the Client named in the respective order. It is an essential part of the contract between the parties and becomes incorporated into the contract between the parties by reference.

1. Preambel

1.1 The Contractor provides a software platform for the digital representation of process documentation in manufacturing companies and for linking it to existing IT systems. The parties have concluded a contract which includes the processing of personal data by the Contractor on behalf of the Client ("Main Contract").

1.2 This Data Processing Agreement ("DPA") specifies, as part of the Main Contract, the obligations of both parties to comply with the applicable data protection law, inparticular the requirements of the EU Data Protection Regulation ("GDPR").

2. Scope

The Contractor processes personal data on behalf of the Client. The subject-matter of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects are specified in the Main Contract and in **Appendix 1**. The term of this DPA shall depend on the term of the Main Contract.

3. Instructions

3.1 The Contractor may only process personal data within the scope of the order and the documented instructions of the Client. The instructions shall initially be set out in the Main Contract and may subsequently be amended, supplemented or replaced by the Client in text form. Verbal instructions must be confirmed immediately by the Client in text form.

3.2 If the Contractor is obliged to process personal data in accordance with the law of the Union or the Member State to which the Contractor is subject, the Contractor shall inform the Client thereof in writing prior to such processing, unless the law prohibits such information for important reasons of public interest. In the latter case, the Contractor shall inform the Client without delay as soon as legally possible.

3.3 The Contractor shall inform the Client without delay if it believes that an instruction violates applicable laws. The Contractor may suspend the implementation of the instruction until it has been confirmed or amended by the Client.

4. Technical and Organizational Measures

4.1 The Contractor undertakes towards the Client to comply with the technical and organizational measures required to comply with the applicable data protection regulations. This includes in particular the requirements of Art. 32 GDPR.

4.2 The status of the technical and organizational measures existing at the time of conclusion of the contract is documented in **Appendix 2**. The parties agree that changes to the technical and organizational measures may be necessary to adapt to technical and legal conditions. The Contractor reserves the right to change the security measures taken, but it must be ensured that they do not fall below the contractually agreed level of protection. The Client may request an up-to-date overview of the technical and organizational measures taken by the Contractor at any time.

5. Data Subject Rights

5.1 The Contractor shall, taking into account the nature of the processing, assist the Client by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Client's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR (in particular access, correction, blocking or deletion). To the extent that the assistance of the Contractor is necessary for the protection of rights of data subjects by the Client, the Contractor shall take the necessary measures according to the instructions of the Client. Taking into account the nature of the processing, the

Contractor shall, insofar as possible, assist the Client by appropriate technical and organizational measures to enable the Client to fulfill its obligations to respond to data subject requests.

5.2 The Contractor may only provide information to third parties or to data subjects with the prior consent of the Client. It shall forward requests addressed directly to the Contractor to the Client without undue delay.

6. Other Obligations of the Contractor

6.1 The Contractor shall inform the Client immediately, at the latest within 48 hours, if it becomes aware of violations of the protection of personal data processed on behalf of the Client.

6.2 The Contractor shall support the Client in preparing and updating the records of processing activities regarding the data processing performed by the Contractor on behalf of the Client, and, if necessary, in carrying out a data protection impact assessment. All necessary information and documentation must be made available to the Client immediately upon request.

6.3 If the Client is subject to an audit by a supervisory authority or other parties or if a data subjects requests to exercise its rights against the Client, the Contractor undertakes to support the Client to the necessary extent insofar as the personal data processed on behalf of the Client is affected.

6.4 The persons employed by the Contractor for the processing have committed themselves in writing to confidentiality, have been made familiar with the relevant provisions of all relevant data protection laws and are continuously appropriately instructed and monitored with regard to the fulfilment of data protection requirements.

6.5 The Contractor shall support the Client in complying with the obligations set out in Articles 32 to 36 GDPR, taking into account the type of processing and the information available to the Contractor.

6.6 The Client can contact the Contractor's data protection officer at any time if there should be any questions about data protection at the Contractor. The Contractor’s data protection officer is Christian Schmoll (Tel. +49 (0)89 4622 7322, e-mail schmoll@dp.institute).

7. Rights and Obligations of the Client

7.1 The Client shall be responsible for assessing the lawfullness of the data processing and for safeguarding the rights of data subjects.

7.2 The Client shall be entitled to monitor and audit compliance with the regulations on data protection and the contractual agreements at the Contractor to a reasonable extent itself or through third parties, in particular by obtaining information and inspecting the stored data and the data processing programs. The persons entrusted with the control are to be granted access and insight by the Contractor as far as necessary and possible. The Contractor is obliged to provide the necessary information, to demonstrate procedures and to keep records which are necessary for the performance of an audit. Audits at the Contractor's premises must be carried out without any avoidable disruption of the Contractor’s business operations. Unless otherwise indicated for urgent reasons to be documented by the Client, audits shall take place after reasonable advance notice and during the business hours of the Contractor and not more frequently than every 12 months.

8. Sub-Processors

8.1 The Contractor may only use sub-processors with the consent of the Client. The Client consents to the usage of sub-processors in accordance with the List of Sub-Processors attached as **Appendix 3**. The List of Sub-Processors also defines the process for future changes of Sub-Processors.

8.2 The Contractor shall carefully select the sub-processors and shall check prior to the assignment that they can comply with the agreements made between the Client and the Contractor. In particular, the Contractor shall check that all sub-processors have taken the technical and organizational measures as required under Art. 32 GDPR to protect personal data.

8.3 Services which the Contractor uses with third parties as a pure ancillary service in order to carry out its business activities shall not be considered sub-proceessing in the context of this DPA. This includes, for example, cleaning services, pure telecommunications services without concrete reference to services provided by the Contractor for the Client, postal and courier services, transport services and security services.

8.4 The usage of sub-processors shall not affect the Contractor's contractual and data protection obligations towards the Client. The Contractor shall be liable for any acts or omissions of its sub-processors as if they were its own acts or ommissions.

9. Data Transfer to Third Countries

Data is also processed by the Contractor in third countries (outside of the EU/EEA). The transfer of personal data to a third country by the Contractor is carried out on the basis of an adequacy decision in accordance with Art. 45 GDPR and/or on the basis of appropriate safeguards in accordance with Art. 46 GDPR (e.g. Standard Contract Clauses issued by the Commission and concluded between the Contractor and the sub-processor in a third country).

10. Deletion and Return of Personal Data

10.1 Copies of the personal data processed on behalf od the Client shall not be made without the knowledge of the Client, except for backup copies that are necessary to guarantee proper data processing, as well as data which are necessary with regard to compliance with statutory retention obligations.

10.2 Upon termination of the Main Contract or earlier upon request by the Client, the Contractor shall hand over to the Client the personal data or delete the personal data in accordance with data protection laws.

10.3 Documentation which serves as proof of the proper processing of data in accordance with the order shall be stored by the Contractor beyond the end of the contract in accordance with the requirements of applicable data protection laws and regulations.

11. Miscellaneous

11.1 If the data of the Client processed by the Contractor should be endangered by measures of third parties (e.g. by seizure or confiscation), by insolvency proceedings or by other events, the Contractor shall inform the Client immediately. The Contractor shall notify the creditors without delay of the fact that the data are processed on instruction of a third party.

11.2 Ancillary agreements must be made in writing. Should individual parts of this DPA be invalid, this shall not affect the validity of the remaining provisions of the DPA.

Appendix 1: Description of the Data Processing

1. Subject-Matter, Nature and Purpose of the Processing

The Client as the controller uses the Operations 1 Software to digitally map process documentation, connect it to existing IT systems and carry out analyses of the work processes. Personal data is processed for the purpose of performing the services of the Contractor agreed in the Main Contract.

2. Categories of Data Subjects and Types of Personal Data

The personal data processed on behalf of the Client concern users of the Operations1 Software (regularly employees of the Client who access the Operations1 Software in the course of their work).

The personal data processed on instruction of the Client relates to the following categories of data:

- Username;
- Password;
- Name and surname;
- Job title;
- E-mail address;
- Date of birth;
- Preferred language;
- Data on the use of the software platform (e.g. input values or time stamps when using checklists and work instructions and data for processing tasks/tasks);
- Other data provided to the Contractor by the Client for the performance of its services or collected by the Contractor for the Client in the course of the performance of the Contractor's services.

The personal data processed on behalf of the Client regularly does not include special categories of personal data according to Art. 9 GDPR (e.g. health data), unless such special categories of personal data are made available to the Contractor by the Client for the purpose of performing the Contractor's services or are collected by the Contractor in the course of performing its services on the instructions and on behalf of the Client.

3. Duration of Processing

The duration of the processing corresponds to the duration of the Main Contract.

Appendix 2: Technical and Organizational Measures

The following technical and organizational measures are implemented by the Contractor:

1. CONFIDENTIALITY

1.1 Physical Access Control

Hosting/Data Center:

The Operations 1 Software is hosted in a Microsoft Azure data center in the EU.

A detailed documentation of the technical and organizational data security measures taken by Microsoft Azure and Microsoft Azure's certifications in the field of information security (including ISO 27001) can be found here:
https://docs.microsoft.com/en-us/azure/security/fundamentals/overview

Offices:

The offices of the Contractor are located in a technology center in Augsburg and an office building in Frankfurt/Main.

Access to the Contractor's offices is closed day and night. Only the employees of the Contractor have access to the Contractor’s offices in the office building in Frankfurt, in the Technology Center in Ausgburg also guests may have access, but guests must register at the reception.

The Technology Center in Ausgburg uses an electronic locking system managed by the landlord. In the office building in Frankfurt there is an analogue locking system. Key allocation and key management follows a defined process that regulates the granting or withdrawal of access authorizations for rooms both at the beginning and end of an employment relationship.

Access authorizations are only granted to an employee if this has been requested by the respective supervisor/manager. When granting authorizations, the principle of necessity is taken into account.

Visitors may not move freely in the office rooms without escort.

1.2 System Access Control

To gain access to IT systems, users must have appropriate access authorization. For this purpose, corresponding user authorizations are assigned by administrators. This, however, only if this has been requested by the respective supervisor/manager.

The user then receives a user name and an initial password, which must be changed the first time he or she logs on. The password specifications include a minimum password length of 8 characters, whereby the password must consist of upper/lower case letters, numbers and special characters.

Incorrect login attempts are logged. If the password is entered incorrectly 3 times, the login screen is blocked for a short time.

Remote access to Contractor’s IT systems is always via encrypted connections.

An intrusion prevention system is in use on Contractor’s servers. All server and client systems are equipped with anti-virus software, which guarantees a daily supply of signature updates.

All servers are protected by firewalls, which are constantly maintained and supplied with updates and patches.

The access of servers and clients to the Internet and the access to these systems via the Internet is also secured by firewalls. This also ensures that only the ports required for the respective communication can be used. All other ports are blocked accordingly.

All employees are instructed to lock their IT systems when they leave them.

Passwords are always stored encrypted.

1.3 Data Access Control

The access right for Contractor’s IT systems and applications are set up exclusively by administrators. Authorizations are always assigned according to the need-to-know principle. This means that only those persons who maintain and service data, databases or applications or are active in development are granted access rights to data, databases or applications.

The prerequisite is a corresponding request for authorization for an employee by a supervisor/manager.

There is a role-based authorization concept with the possibility of differentiated assignment of access authorizations, which ensures that employees receive access rights to applications and data depending on their respective area of responsibility and, if necessary, on a project basis.

All employees are instructed to deposit information containing personal data and/or information about projects in the designated destruction containers.

Employees are strictly prohibited from installing unauthorized software on IT systems.

All server and client systems are regularly updated with security updates.

1.4 Separation Control

All IT systems used by Contractor for clients are multi-client capable. The separation of data from different clients is always guaranteed.

1.5 Encryption

Administrative access to server systems is always done via encrypted connections. In addition, data on server and client systems is stored on encrypted data carriers. Appropriate hard disk encryption systems are in use.

2. INTEGRITY

2.1 Input Control

The entry, modification and deletion of personal data processed by the Contractor on behalf of the Client are logged with time stamp and user account or the last event is recorded. For example: "Order last updated on AB of XY".

Employees are obliged to always work with their own accounts. User accounts may not be shared or shared with other persons.

2.2 Transfer Control

Any disclosure of personal data on behalf of the Contractor's clients may only take place to the extent agreed with the client and to the extent necessary to provide the contractual services to the client.

All employees working on a client project are instructed with regard to the permissible use of data and the modalities of data transfer.

As far as possible, data will be transmitted to recipients in encrypted form.

The Contractor’s employees are prohibited from using private data carriers in connection with client projects.

All Employees receive regular training on data protection issues. All employees are obliged to handle personal data confidentially.

3. AVAILABILITY AND RESILIENCE

Data on the Contractor’s server systems is backed up incrementally at least daily and "fully" weekly. The backup media are encrypted.

The import of backups is tested regularly.

The IT systems have an uninterruptible power supply. A fire alarm system and a CO2 extinguishing system are located in the server room. All server systems are subject to monitoring, which immediately triggers reports to an administrator in case of malfunctions.

The Contrator implemented and maintains a detailed emergency plan, which also includes a business continuity and restart plan.

4. ORDER CONTROL

The Contractor designated a data protection officer. When external service providers or third parties are involved, a data processing agreement is concluded in accordance with the applicable data protection laws, following a prior audit. Sub-processors are also regularly audited during the contractual relationship.

5. PRIVACY BY DESIGN AND PRIVACY BY DEFAULT

It is ensured that the principle of necessity is already taken into account in connection with user interfaces during the development of the Software. For example, form fields and screen masks can be designed flexibly. For example, mandatory fields can be provided or fields can be deactivated.

6. PROCEDURES FOR REGULAR REVIEW, ASSESSMENT AND EVALUATION

The Contractor implemented a comprehensive data protection management system, including detailed policies on data protection and information security.

A Data Protection and Information Security Team has been established to plan, implement, evaluate and adjust measures in the area of data protection and information security. All implemented measures and all policies are regularly evaluated and adjusted with regard to their effectiveness.

In particular, it is ensured that data protection incidents are recognized by all employees and are reported to the Data Protection and Information Security Team without undue delay. The Data Protection and Information Security Team will immediately investigate every incident. If data is affected that are processed on instruction of clients, it is ensured that the respective clients are informed about the type and extent of the incident immediately.

Appendix 3: List of Sub-Processors

The Contractor shall use the following Sub-Processors to provide the services under the Main Contract:

Sub-Processor	Services	Location of Processing	Appropriate Safeguards (Art. 46 GDPR)
Microsoft Deutschland GmbH, Germany	Hosting of the Operations1 Software („MS Azure“)	EU	n/a
ActiveCampaign, LLC, USA	Sending push e-mails, optionally connectable to the Operations1 Software	USA	Certification under the EU-U.S. Data Privacy Framework (Adequacy Decision) and additionally Standard Contractual Clauses
Intercom R&D Unlimited Company, Ireland	Helpdesk, Live Chat, Forwarding of support requests	EU, USA	Certification under the EU-U.S. Data Privacy Framework (Adequacy Decision) and additionally Standard Contractual Clauses
Ynoox LLC/GmbH, Switzerland	Conversion and modification of PDF reports	EU	n/a
CarboneIO SAS, France	Creation of customised PDF reports	EU	n/a

Contractor may terminate the assignment of individual subcontractors or assign additional subcontractors. When contracting additional subprocessors, Contractor shall inform the Client by electronic means at least 30 days before the additional subprocessor is to be used of its intended use. Excepted from this are emergency replacements as defined below. If the Client has a substantial reason to object to the use of a subcontractor, the Client shall notify Contractor in writing, stating the substantial reason, no later than 15 days after the notification of the planned use of the subcontractor. If the Client does not object within this period, the use of the additional sub-processor shall be deemed to be the approved by Client.

Should the Client object, the Contractor can remedy the objection as follows: (1.) The Contractor will not use the additional sub-processor to process personal data of the Client, or (2.) the Contractor will take measures to eliminate the material reason for the objection of the Client, or (3.) the Contractor may temporarily or permanently cease to provide the aspect of the service to the Client that is affected by the use of the additional sub-processor and refund to the Client any remuneration already paid in advance for the provision of the aspect of the service. If none of these three options should be feasible and the objection was not remedied within 15 days after receipt of the objection, each party can terminate the contract extraordinarily with appropriate period of notice.

Emergency replacements of a sub-processor may become necessary if the need for the immediate deployment of an additional sub-processor is beyond the control of Contractor, for example, if a sub-processor unexpectedly ceases operations or breaches its material contractual obligations to Contractor so that Contractor is/would no longer be able to perform the service owed to the Client. In such a case, Contractor will immediately inform the Client of the additional sub-processor and the objection process, as defined above, will be initiated with the Client's notification.