Data Processing Agreement pursuant to Article 28, para. 3 DS-GVO [General Data Protection Regulation]

Client (responsible party)

See registration of the user

Contractor (order processor):
Ingentis Software Development GmbH
Raudtener Str. 7
D-90475 Nürnberg

1 Subject matter and duration of the Agreement

- See Appendix A -

The Contractor processes personal data for the Client pursuant to Article 4, No. 2 and Article 28 DS-GVO under the terms of this Contract.

The contractually-agreed service is to be provided exclusively in a member state of the European Union or in a state party to the Agreement on the European Economic Area. Any relocation of the service or sub-operations thereof to a third-party country requires the Client's prior consent and is allowed only if the specific prerequisites of Article 44 et seq. DS-GVO are fulfilled (e.g. adequacy decision by the Commission, standard data protection clauses, approved codes of conduct).

Duration of the Contract
The Contract is concluded for an indefinite period. The period of notice is one month to the end of the quarter. The Client can terminate the Contract at any time without notice if the Contractor is in serious breach of the data protection regulations or the provisions of this Contract, the Contractor is unable to or does not intend to follow an instruction given by the Client or the Contractor denies the Client's supervisory rights contrary to the terms of the Contract. In particular, failure to fulfil the obligations agreed under this Contract and ensuing from Article 28 DS-GVO constitute a serious infringement.

2 Type and purpose of processing, type of personal data and categories of affected persons:

- See Appendix B -

3 Rights and obligations and authority to issue directives on the part of the Client

The responsibility for assessing the reliability of processing in accordance with Article 6, para. 1 DS-GVO, and also for safeguarding the rights of the affected persons pursuant to Articles 12 to 22 DS-GVO lies solely with the Client. Nonetheless, the Contractor is under an obligation to forward all associated inquiries, insofar as they are directed to the Client, to said Client.

Changes to the subject matter of the processing activity and procedural changes must be agreed jointly between Client and Contractor and defined in writing or in a documented electronic format.

As a rule, the Client issues all orders, partial orders and instructions in writing or in a documented electronic format. Verbal instructions must be confirmed immediately in writing or in a documented electronic format.

The Client is entitled to make certain, as defined under para. 5, prior to the start of processing and thereafter on a regular basis in an appropriate manner, that the technical and organizational measures implemented by the Contractor, and also the obligations defined in this Contract, are being observed.

The Client shall notify the Contractor immediately if it discovers defects or irregularities during the review of the order results.

The Client is under an obligation to treat all knowledge of business secrets and data security measures of the Contractor gained under the terms of the contractual relationship as confidential. This obligation shall remain in place even after the Contract has been terminated.

4 Client's parties authorized to issue directives

The customer's individuals authorized to issue directives are those users of the application who are registered as editors.

Any change of or longer-term incapability of the contact persons will be communicated to the Contractor immediately in electronic format. The directives must be retained for their validity period and for three full calendar years thereafter.

5 Obligations on the part of the Contractor

The Contractor processes personal data exclusively under the terms of the agreements made and in accordance with the Client's directives unless under an obligation to process in an alternative manner in accordance with the law of the European Union or of the member states with which the order processor has to comply (e.g. determinations of law enforcement or state protection authorities); in such a case, the order processor shall communicate to the responsible party these legal requirements, unless the right concerned forbids such notification on account of an important public interest (Article 28, para. 3, sentence 2, lit. a DS-GVO).

The Contractor shall not use the personal data provided for processing for any other purposes, especially its own. Copies or duplicates of the personal data shall not be created without the Client's knowledge.

The Contractor guarantees the contractual processing of all agreed measures for the contractual processing of personal data. The Contractor guarantees that the data processed for and on behalf of the Client is strictly separated from other data pools.

The data carriers originating from the Client and/or used for the Client are specially identified. Entry and exit and ongoing use are documented.

Upon fulfilment of the rights of the affected persons pursuant to Articles 12 to 22 DS-GVO by the Client, upon the creation of directories of processing activities, and also in case of required data protection impact assessments by the Client, the Contractor must cooperate to the extent required and provide the Client with appropriate support wherever possible (Article 28, para. 3, sentence 2 lit e and f DS-GVO).

The Contractor will notify the Client immediately if it believes that a directive issued by the Client is in breach of statutory provisions (Article 28, para. 3, sentence 3 DS-GVO). The Contractor shall be entitled to suspend the implementation of the directive concerned until it has been confirmed or amended by the Client's responsible party following a review.

The Contractor must correct, delete or limit the processing of personal data ensuing from the contractual relationship if the Client so demands by way of a directive and no legitimate interests of the Contractor stand contradictory.

The Contractor is allowed to disclose information about personal data ensuing from the contractual relationship to third parties or the party concerned only after the Client has issued a directive or granted its consent.

The Contractor agrees that the Client shall be entitled - essentially by prior arrangement - to monitor compliance with the provisions on data protection and data security, as well as the contractual agreements to an extent that is both reasonable and necessary, or to have such compliance monitored by a third party assigned by the Client, specifically by collecting information and inspecting the stored data and the data processing programs, and also by means of reviews and inspections on the premises

(Article 28, para. 3, sentence 2 lit. h DS-GVO). The Contractor gives its assurance that it will provide the support required during such monitoring activities.

The Contractor confirms it has knowledge of those data protection provisions of the DS-GVO that are relevant for order processing. The Contractor also undertakes to comply with the privacy protection regulations relevant to this order, which the Client must observe (e.g. banking secrecy, secrecy of telecommunications, secrecy of social data, professional secrecy pursuant to Section 203 StGB [German Penal Code], etc.)

The Contractor undertakes to maintain confidentiality for the contractual processing of the Client's personal data. This obligation shall remain in place even after the contract has been terminated.

The Contractor gives its assurance that it will make the employees who carry out the work, before commencement of the activity, aware of the data protection provisions relevant to them and will obligate such employees to maintain confidentiality by suitable means for the period of their activity and also after the employment relationship has been terminated (Article 28, para. 3, sentence 2, lit. b and Article 29 DSGVO). The Contractor shall monitor compliance with the data protection provisions within its operation**.**

The appointed Data Protection Officer for the Contractor is:

Mr. Michael Gruber
BSP-SECURITY
Thundorferstr. 10
D-93047 Regensburg
email: michael.gruber@bsp-security.de

6 Contractor's reporting obligations in case of disruptions during processing and personal data protection breaches

The Contractor shall immediately communicate to the Client any disruptions, breaches by the Contractor or persons employed by the Contractor, and also against data protection provisions or against the stipulations made in the order, as well as any suspicion of data protection breaches or irregularities during the processing of personal data. This applies also for any reporting and notification obligations of the Client pursuant to Articles 33 and 34 DS-GVO. The Contractor guarantees to help the Client meet its obligations pursuant to Articles 33 and 34 DS-GVO by means of appropriate support (Article 28, para. 3, sentence 2 lit. f DS-GVO). The Contractor may issue notifications pursuant to Article 33 or 34 DS-GVO for the Client only after a prior directive in accordance with Item 4 of this Contract.

7 Sub-contractual relationships with sub-contractors (Article 28, para. 3, sentence 2 lit. d DS-GVO)

The Contractor is permitted to assign contractors to process the Client's data only with the Client's consent, Article 28, para. 2 DS-GVO, such consent having to be granted through one of the aforementioned communication channels (Item 4), the exception being verbal consent. The consent can be granted only if the Contractor provides the Client with the name, address and proposed activity of the sub-contractor. Moreover, the Contractor must ensure that it carefully selects the sub-contractor with special consideration for the suitability of the technical and organizational measures taken by said sub-contractor as defined by Article 32 DS-GVO. The relevant review records must be presented to the Client on request.

Any assignment of sub-contractors in third-party country requires the Client's prior consent and is allowed only if the specific prerequisites of Article 44 et seq. DS-GVO are fulfilled (e.g. adequacy decision by the Commission, standard data protection clauses, approved codes of conduct).

The Contractor must contractually ensure that the provisions agreed between Client and Contractor also apply vis-à-vis sub-contractors. In the contract with the sub-contractor, the details must be specified in such a manner that the responsibilities of the Contractor are clearly delimited from those of the sub-contractor. If several sub-contractors are used, this applies also to the responsibilities between the sub-contractors. In particular, the Client must be entitled to conduct appropriate reviews and inspections, also on-site, at sub-contractors or have such reviews and inspections conducted by a third party assigned by the Client.

The Contract with the sub-contractor must be drawn-up in writing, electronic format also suffices (Article 28, para. 4 and para. 9 DS-GVO).

Data can be transmitted to the sub-contractor only if the sub-contractor has fulfilled the obligations pursuant to Articles 29 and 32, para. 4 DS-GVO with respect to its employees.
The result of the reviews must be documented and made accessible to the Client upon request.

The Contractor is liable to the Client for ensuring that the sub-contractor meets the data protection obligations contractually imposed by the Client in accordance with this section of the Contract.

Currently, the sub-contractors designated in Appendix C by name, address and contractual content are assigned to process personal data to the extent described therein. The Client agrees to such assignment.

The order processor shall always inform the party responsible about any intended change concerning the addition of new or replacement of existing sub-contractors, thereby giving the Client the opportunity to object to such changes (Section 28, para. 2, sentence 2 DS-GVO).

The sub-contractors assigned to complete the required tasks are listed in Appendix C.

8 Technical and organizational measures pursuant to Article 32, DS-GCO (Article 28, para. 3, sentence 2 lit. c DS-GVO)

For the specific order processing, a protection level commensurate with the risk to the rights and freedoms of the natural persons affected by the processing activities shall be guaranteed. For this purpose, the protection goals of Article 32, para. 1 DS-GVO, such as confidentiality, integrity and availability of systems and services, as well as the resilience thereof with respect to type, scope, circumstances and purpose of the processing activity, are considered in such a way that the risk is permanently reduced by suitable technical and organizational remedial measures.

For the contractual processing of personal data, the following methodology, which considers the probability of occurrence and severity of the risks to the rights and freedoms, is applied to conduct the risk assessment:

- Risk analysis

The regular review, assessment and evaluation of the efficiency of the technical and organizational measures described in Appendix D by the Client is
stipulated as binding to guarantee processing in compliance with data protection regulations.

Proof through certification can be furnished as follows:
The Contractor must conduct a review, assessment and evaluation of the efficiency of the technical and organizational measures for guaranteeing secure processing as and when required, but at least once annually (Article 32, para. 1 lit. d DS-GVO). The result, including a full audit report, must be communicated to the Client.

Decisions on the organization of data processing and on the applied procedures that are significant to security must be taken jointly between Contractor and Client.

Insofar as the measures implemented on the Contractor's do not satisfy the Client's requirements, the Contractor shall notify the Client without delay.

The measures implemented on the Contractor's premises can be modified during the course of the contractual relationship to keep abreast of technical and organizational advancements, but must not fall below the agreed standards.
The Contractor must agree significant modifications with the Client in documented format (writing, electronic). Such agreements must be retained for the duration of this Contract.

9 Contractor's obligations on termination of the Contract, Article 28, para. 3, sentence 2 lit. g DS-GVO

On completion of the contractual activities, the Contractor must hand to the Client all data, documents and prepared processing or usage results associated with the contractual relationships which are its possession and located on sub-contractors' premises.

The Contractor must delete and/or destroy any copies in compliance with data protection law. Such deletion and/or destruction must be confirmed to the Client in writing or in a documented electronic format with the date stated.

10 Liability

Article 82 DS-GVO refers. The following is always agreed:

11 Miscellaneous

Agreements on the technical and organizational measures, as well as monitoring and review documents (including for sub-contractors) must be retained by both contracting parties for their validity period and for three full calendar years thereafter.

Side agreements must always be in writing or a documented electronic format.

The Contractor must notify the Client immediately if the ownership of the Client's personal data to be processed on the Contractor's premises is jeopardized by third-party measures (such as attachment of seizure), through insolvency or composition proceedings or by other such events.

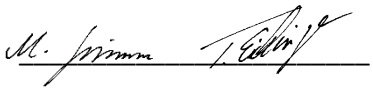
Any objection to the right of retention pursuant to Section 273 BGB [German Civil Code] with respect to the data processed for the Client and the associated data carriers is ruled out.

If individual parts of this Agreement are ineffective, the validity of the Agreement as a whole shall not be affected.

The Client consents to the provisions of this Contract through electronic confirmation.

The confirmation is will be added to the Client's registration data with date and time.

Nuremberg

_____ 

Place, Contractor

Appendix A

Subject matter and duration of the Agreement

The order comprises the following:

Ingentis orginio, SaaS solution for depicting personnel structures in organization charts
Maintenance and consulting services, product training

- Provisioning and hosting of the orginio software (with the involvement of sub-contractors), which depicts data from organization structures and personnel master records in the form of organization charts and lists.
- Software maintenance: Regular importing of software releases (orginio). Processing of reported support cases. In certain cases, it may be necessary to access the Client data in orginio in order to analyze reported problems. In this case, the Client will be asked to set-up temporary access to the software
- Optionally on the basis of a separate assignment: Support for the configuration & operation of the software, and also importing of the data.

(Subject matter of the order, description of services)

Appendix B

Type and purpose of processing, type of personal data and categories of affected persons:

Processing of personnel data of the Client's employees for graphically displaying the data in organization charts, as well as software maintenance, consulting and support

Type:
☐ local
☒ remote

(more detailed description, reference to specification as Appendix, etc.)

Type of personal data (according to definition of Article 4, No. 1, 13, 14 and 15 DSGVO):

- ☒ Personnel master data
- ☒ Communication data (e.g. phone, email)
- ☐ Contract master data (contractual relationship, product and/or contract interest)
- ☐ Client history
- ☒ Contract billing and payment dat
- ☒ Performance and conduct data
- ☐ Planning and control data
- ☐ Report data (from third parties, e.g. credit agencies, or from public directories)
- ☐ Health data
- ☐ Genetic data
- ☐ Biometric data
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____

Categories of affected persons (according to the definition of Article 4, No. 1 DS-GVO):

☒ The categories of persons affected by the processing activity include:

- ☐ Clients
- ☐ Prospects
- ☐ Subscribers
- ☒ Employees
- ☐ Suppliers
- ☐ Commercial agents
- ☐ Applicants
- ☐ Business partners
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____

Appendix C

Approved sub-contractors

#1 Sub-contractors	RZ Hetzner Online (ISO/IEC 27001 certified)	
Subject matter of the order	Data types and categories	Group of affected parties
Local support for administration (Helping Hands)	None, support only in the computer center	Support only in the computer center

#2 Sub-contractors	LogMeIn Ireland Ltd., Bloodstone Building Block C, 70 Sir John Rogerson´s Quay, Dublin 2, Ireland	
Subject matter of the order	Data types and categories	Group of affected parties
Support software for holding Online Meetings	None	Only provision of software for screen transmission

#3 Sub-contractors	Markos Tafakis (ext. service provider) headquartered in Nuremberg	
Subject matter of the order	Data types and categories	Group of affected parties
Sales and Consulting	According to Appendix B	According to Appendix B

#4 Sub-contractors	TeamViewer GmbH, Jahnstr. 30, 73037 Göppingen	
Subject matter of the order	Data types and categories	Group of affected parties
Support software for holding Online Meetings	None	Screen transmission

#5 Sub-contractors	Amazon Web Services Inc., 410 Terry Ave North, Seattle, WA 98109-5210, US	
Subject matter of the order	Data types and categories	Group of affected parties
Local support for administration (Helping Hands)	None, support only in the computer center	Support only in the computer center

# 6 Subcontractor	Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18	
Object of agreement	Data types and categories	Group of affected persons
Microsoft Teams Microsoft Skype for Business Microsoft Exchange Microsoft Onedrive Micrsoft 365 Microsoft SharePoint Microsoft Azure	In accordance with Appendix B	In accordance with Appendix B

Appendix D
Technical and organizational measures (TOM) pursuant to Article 32 DS-GVO

1 Objective

The intention and obligation of the management of Ingentis Softwareentwicklung GmbH is to comply with all statutory provisions concerning data protection and to protect the personal rights of each and every individual. This concerns every job candidate and employee, as well as clients, suppliers and business partners. Moreover, the object of the management is to protect the company's data. All employees of Ingentis Softwareentwicklung GmbH are obliged by policies to meet such objectives. The managers shall ensure compliance with these policies within their department.

The information security measures are geared to the requirements of Article 32 DS-GVO.

2 IT Security Policies

The company has a comprehensive and binding set of regulations for handling data and IT systems. Special stipulations are made on the following issues:

- Network infrastructure (internal, external, LAN, WAN, WLAN)
- Password policy
- Authorization management
- Use of email and the Internet
- Use of software
- Handling company and client data
- External access to the LAN
- …

Every employee is obligated in writing to comply with the IT Security Policies.

3 Data Protection Officer

For Ingentis Softwareentwicklung GmbH,

Mr. Michael Gruber
BSP-SECURITY
Thundorferstr. 10
D-93047 Regensburg
email: michael.gruber@bsp-security.de

has been appointed in writing as the external Data Protection Officer (eDPO). The Data Protection Officer shall perform all the duties incumbent upon him pursuant to the DS-GVO.

3.1 Obligation

All employees of Ingentis Softwareentwicklung GmbH are obliged, upon being hired, to maintain confidentiality pursuant to Article 28, para. 3 lit. b, Article 39, para. 1 lit. a DS-GVO and to Section 88 TKG (Secrecy of Telecommunications Act)

Employees are sensitized to and trained in the requirements for data protection by means of instructions and information.

3.2 Order Data Processing pursuant to Article 28 DS-GVO

Upon assignment of an order, Ingentis Softwareentwicklung GmbH processes, collects or uses personal data on behalf of the client pursuant to Article 28 DS-GVO. The purpose of the contractual relationship includes the processing of personal data in accordance with the concluded main contract. The agreement on order processing pursuant to Article 28 DS-GVO governs the protection of personal data as they are being processed on behalf of another party.

Ingentis Softwareentwicklung GmbH shall assist the Client with meeting data protection obligations, especially with respect to notification, provision of information, correction, blocking and deletion, to the best of its ability. Any sub-contractors assigned through necessity shall be obligated to the same data protection regulations as those set out in client AV contracts. Sub-contractors must implement suitable technical and organizational measures in such a manner that processing complies with the requirements of the Data Protection Act.

3.3 Data protection documentation

I have created, and where necessary updated, the following data protection documents:

- Directory of processing activities (Article 30 DS-GVO)
- Technical and organizational measures pursuant to Article 32 DS-GVO

4 Technical and organizational measures (Article 32 DS-GVO)

1 Non-disclosure (Article 32, para. 1 lit. b DS-GVO)

Access control No unauthorized access to data processing systems	Measures for denying unauthorized persons access to the data processing systems used to process and use personal data: • *Key with key handover record* Employees can be identified by a unique number on the key. A record is automatically created when a key is assigned via the programming software provided for this purpose. • *Security locking cylinder* The doors are equipped with a security locking cylinder with programmable chip keys. • *Locking system, server room* Server rooms are fitted with electronic locking systems and keys are accessible to only a highly-restricted group of people. • Visitors are received in the reception entrance area and are not granted access to computer systems. • Outdoor video surveillance.
Access control No unauthorized reading, copying, editing or deleting within the system	Measures to guarantee that the parties authorized to use a data processing system are able to access only those data allowed under their access authorization, and that personal data cannot be read, copied, edited or deleted by unauthorized parties during processing and use and after storage: The data we receive to verify problems or errors within our applications are stored in special directories to which only authorized employees have access. These data are automatically deleted once the problem has been rectified. An authorization concept is generally in place for ensuring that each employee has access only to those data they require for their projects. The authorizations can be changed at short notice at any time by system administrators. Access from outside is prevented by firewall systems. External data connections are protected by VPN technology.
Separation control Separate processing of data collected for different purposes	Measures to guarantee that data collected for different purposes can be processed separately: Client-controlled applications

	Client-controlled applications with purpose-built mechanisms
Pseudonymization The processing of personal data such that these data can no longer be assigned to a specific affected person without using additional information, insofar as this additional information can be kept separate and are subject to corresponding technical and organizational measures; (Article 32, para. 1 lit. a DS-GVO; Article 25, para. 1 DS-GVO)	Pseudonymized personal data are used wherever possible.

2 Integrity (Article 32, para. 1 lit. b DS-GVO)

Transmission control No unauthorized reading, copying, editing or deleting during electronic transmission or transport	Measures to guarantee that personal data cannot be read, copied, edited or removed by unauthorized parties as such data are being transmitted or saved to data carriers, and that it is possible to check and establish the locations to which transmission of personal data is envisaged through data transmission facilities: Personal data are transmitted only in consultation with the owner (e.g. Client) of such data. In this case, data are transmitted exclusively as agreed with the owner. Generally speaking, data can be transmitted in encrypted format and secured accordingly via VPN connections.

Input control Establishing whether and by whom personal data have been entered into data processing systems, edited in or deleted from such systems	Measures to guarantee the facility to verify and establish whether and by whom personal data have been entered into data processing systems, edited in or deleted from such systems: Events are logged on special systems (operating systems, firewall and VPN dial-in).

3 Availability and capacity (Article 32, para. 1 lit. b DS-GVO)

Availability control	System with RAID Local emergency power supply (UPS) Backup system (the backup tapes are securely stored outside of the company) Firewall Virus protection Regular patching of operating systems and applications
Fast recoverability (Article 32, para. 1 lit. c DS-GVO)	The recovery of backup data is tested by restore checks.

4 Procedure for regular reviews, assessment and evaluation (Article 32, para. 1 lit. d DS-GVO; Article 25, para. 1 DS-GVO)

Incident Response Management	A special reporting process that informs the affected parties and the supervisory authority in case of a security incident is being modeled and implemented.
Privacy-Enhancing Presets (Article 25, para. 2 DS-GVO	Consideration is given to the principles of "Privacy by Design" and "Privacy by default" for IT operation and IT development.
Order control	No order processing as defined by Article 28 DS-GVO without an instruction from the Client, i.e.: explicit contractual arrangement, formalized order management, strict service provider selection, duty of pre-conviction, follow-ups.