Data Processing Contract
to
Art. 28 para. 3 GDPR

Client (responsible party)

See registration of the user

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

1 Subject matter and duration of the agreement

- See Appendix A -

The contractor processes personal data for the client within the meaning of
Art. 28 GDPR based on this contract.

Depending on the data center selected (see Annex C), the contractually agreed service is provided in a member state of the European Union or in a state party to the Agreement on the European Economic Area. If the data is processed in a third country in accordance with Annex C, this is only done based on Art. 44 et seq. GDPR. Any relocation of the service or parts thereof to a third country requires the prior consent of the client and may only take place if the special requirements of Art. 44 et seq. GDPR are met (e.g. adequacy decision of the Commission, standard data protection clauses, approved codes of conduct).

Duration of the order
The contract is concluded for an indefinite period. The notice period is one month to the end of the quarter. The Client may terminate the contract at any time without notice in the event of a serious breach of data protection regulations or the provisions of this contract by the Contractor.

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

- See Appendix B -

3 Rights and obligations as well as the client's authority to issue instructions

The client alone is responsible for assessing the permissibility of the processing in accordance with Art. 6 para. 1 GDPR and for safeguarding the rights of the data subjects in accordance with Art. 12 to 22 GDPR. Nevertheless, the Contractor is obliged to forward all such requests to the Client without delay, if they are recognizably addressed exclusively to the Client.

Changes to the object of processing and procedural changes must be jointly agreed between the client and the contractor and specified in writing or in a documented electronic format.

As a rule, the client shall issue all orders, partial orders, and instructions in writing or in a documented electronic format. Verbal instructions must be provided immediately in writing or in a documented electronic format.

The Client shall be entitled to verify compliance with the technical and organizational measures taken by the Contractor and with the obligations set out in this Agreement before the start of processing and then regularly in an appropriate manner as set out in No. 5.

The Client shall inform the Contractor immediately if it discovers errors or irregularities in the inspection of the order results.

The Client is obliged to treat all knowledge of the Contractor's business secrets and data security measures obtained during the contractual relationship as confidential. This obligation shall remain in force even after termination of this contract.

4 Authorized representatives of the client

Persons authorized to issue instructions to the client are the respective users of the application registered as editors.

5 Obligations of the Contractor

The Processor shall process personal data exclusively within the framework of the agreements made and in accordance with the instructions of the Controller, unless the Processor is obliged to do so by the law of the European Union or the Member States to which the Processor is subject (e.g. investigations by law enforcement or state security authorities); in such a case, the Processor shall notify the Controller of these legal requirements prior to processing, unless the law in question prohibits such notification due to an important public interest (Art. 28 para. 3 sentence 2 lit. a GDPR).

The Contractor shall not use the personal data provided for processing for any other purposes, in particular not for its own purposes. Copies or duplicates of personal data shall not be created without the knowledge of the client.

The contractor shall cooperate to the extent necessary in the preparation of the records of processing activities and in any necessary data protection impact assessments of the client and shall provide the client with appropriate support as far as possible (Art. 28 para. 3 sentence 2 lit. e and f GDPR).

To respond to requests to exercise the rights of data subjects in accordance with Art. 12 to 23 GDPR, the Contractor shall support the Client as far as possible with technical and organizational measures.

The Contractor shall inform the Client immediately if, in its opinion, an instruction issued by the Client violates statutory provisions (Art. 28 para. 3 sentence 3 GDPR). The contractor is entitled to suspend the implementation of the corresponding instruction until it is confirmed or amended by the controller at the client after review.

The contractor may only provide information about personal data from the contractual relationship to third parties or the data subject with the prior instruction or consent of the client.

The Contractor agrees that the Client - generally after prior notification - is entitled to check compliance with the provisions on data protection and data security as well as the contractual agreements to the appropriate and necessary extent itself or through third parties commissioned by the Client, by obtaining evidence and through on-site inspections (Art. 28 para. 3 sentence 2 lit. h GDPR). The Contractor warrants that it will assist with these checks where necessary. Evidence may also be provided by means of audit reports or certificates. Commissioned third parties may not be in a direct competitive relationship with the contractor. The inspections must not lead to an excessive impairment of the course of business.

The Contractor undertakes to maintain confidentiality when processing the Client's personal data in accordance with the contract. This obligation shall continue to exist even after termination of the contract.

The Contractor warrants that it will familiarize the employees engaged in the performance of the work with the data protection provisions applicable to them before they commence their work and that they will be bound to secrecy in an appropriate manner for the duration of their work and after termination of the employment relationship (Art. 28 para. 3 sentence 2 lit. b and Art. 29 GDPR). The Contractor shall monitor compliance with data protection regulations in its company.

The Contractor has appointed a data protection officer:

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

6 Notification obligations of the contractor in the event of processing disruptions and personal data breaches

The Contractor shall notify the Client without delay of any disruptions, breaches by the Contractor or the persons employed by the Contractor, breaches of data protection provisions or of the stipulations made in the order, as well as any suspicion of data protection breaches or irregularities in the processing of personal data. This also applies regarding any reporting and notification obligations of the Client pursuant to Art. 33 and Art. 34 GDPR. The Contractor warrants that, if necessary, it will provide the Client with appropriate support in its obligations under Art. 33 and 34 GDPR (Art. 28 para. 3 sentence 2 lit. f GDPR). The Contractor may only carry out notifications pursuant to Art. 33 or 34 GDPR for the Client after prior instruction in accordance with Section 4 of this contract.

7 Subcontracting relationships with subcontractors (Art. 28 para. 3 sentence 2 lit. d GDPR)

At present, the subcontractors specified in Annex C with name, address and order content are engaged in the processing of personal data for the Contractor to the extent specified therein. The client agrees to their commissioning.

The Contractor is permitted to commission other subcontractors to process the Client's data, Art. 28 (2) GDPR, provided that the Contractor informs the Client of this, and the Client does not exercise its right to object within 30 days. The objection is only permissible for objective reasons. To this end, the contractor shall inform the client of the name and address of the subcontractor and the intended activity. In addition, the contractor must ensure that it carefully selects the subcontractor, taking account of the suitability of the technical and organizational measures taken by them within the meaning of Art. 32 GDPR.

Subcontractors in third countries may only be commissioned if the special requirements of Art. 44 et seq. GDPR are met (e.g. adequacy decision by the Commission, standard data protection clauses, approved codes of conduct).

The contractor must contractually ensure that the regulations agreed between the client and contractor also apply to subcontractors.

The Contractor shall be liable to the Client for ensuring that the subcontractor complies with the data protection obligations contractually imposed on it by the Contractor in accordance with this section of the contract.

8 Technical and organizational measures pursuant to Art. 32 GDPR (Art. 28 para. 3 sentence 2 lit. c GDPR)

A level of protection appropriate to the risk to the rights and freedoms of natural persons affected by the processing is ensured for the specific data processing. For this purpose, the protection objectives of Art. 32 para. 1 GDPR, such as confidentiality, integrity and availability of the systems and services as well as their resilience regarding the type, scope, circumstances, and purpose of the processing, are taken into account in such a way that the risk is permanently contained by appropriate technical and organizational measures.

The regular review, assessment, and evaluation of the effectiveness of the technical and organizational measures described in Annex D by the client is mandatory to ensure data protection-compliant processing.

If the measures taken by the Contractor do not meet the Client's requirements, the Contractor shall inform the Client immediately.

The Contractor's measures may be adapted to technical and organizational developments during the contractual relationship but must not fall below the agreed security level.
The Contractor must agree significant changes with the Client in documented form (in writing, electronically). Such agreements must be retained for the duration of this contract.

9 Obligations of the contractor after termination of the contract, Art. 28 para. 3 sentence 2 lit. g GDPR

After completion of the contractual work, the Contractor shall, at the Client's discretion, return to the Client or delete all data, documents and processing or usage results created in connection with the contractual relationship that have come into its possession and to subcontractors, unless there is an obligation to continue storing the data under Union law or the law of the Member States.
Any copies must be deleted or destroyed by the Contractor in accordance with data protection regulations. The deletion or destruction shall be confirmed to the Client in writing or in a documented electronic format, stating the date.

10 Liability

Reference is made to Art. 82 GDPR.

11 Other

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

Should the property or the personal data of the Client to be processed by the Contractor be jeopardized by measures of third parties (such as by seizure or confiscation), by insolvency or composition proceedings or by other events, the Contractor must inform the Client immediately.

The defense of the right of retention within the meaning of § 273 BGB is excluded with regard to the data processed for the client and the associated data carriers.

Should individual parts of this agreement be invalid, this shall not affect the validity of the remainder of the agreement

The client agrees to the terms of this contract by electronic confirmation.

The confirmation is added according to the client's registration data with date and time.

Nuremberg

DocuSigned by: Joachim Rotzinger 58D09928055B4F6...

DocuSigned by: 9E24DCEF963942A...

Location, Contractor

Appendix A

Subject matter, nature and purpose of the processing

The order includes the following:

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

- Provision and hosting of the orginio software (with the involvement of subcontractors), which displays data from organizational structures and personnel master data in the form of organizational charts and lists.
- Software maintenance and further development: regular installation of newer software versions (orginio). Processing of reported support cases. In individual cases, access to the client data in orginio may also be required to analyze reported problems. In this case, the client will be asked to set up temporary access to the software. Analyses may also serve the purpose of further developing the software product.
- Optional based on a separate order: Support with the configuration and operation of the software, as well as the import of data.

(Subject of the contract, description of the services)

Appendix B

type of personal data and categories of data subjects:

Processing of personnel data of the client's employees for the graphical representation of data in organizational charts as well as software maintenance, consulting and support

(more detailed description, reference to service specifications as an attachment, etc.)

Type of personal data (according to the definition of Art. 4 No. 1, 13, 14 and 15 GDPR):

- ☒ Personal master data
- ☒ Pictures
- ☒ Communication data (e.g. telephone, e-mail)
- ☐ Contract master data (contractual relationship, product or contractual interest)
- ☐ Customer history
- ☒ Contract billing and payment data
- ☒ Performance and behavioral data
- ☐ Planning and control data
- ☐ Information (from third parties, e.g. credit agencies, or from public directories)
- ☐ Health data
- ☐ Genetic data
- ☐ Biometric data
- ☐_____
- ☐_____
- ☐_____
- ☐_____

Categories of data subjects (according to the definition of Art. 4 No. 1 GDPR):

☒ The categories of data subjects affected by the processing include

- ☐ Customers
- ☐ Interested parties
- ☐ Subscribers
- ☒ Employees
- ☐ Suppliers
- ☐ Sales representative
- ☐ Applicants
- ☐ Business partner
- ☐_____
- ☐_____
- ☐_____
- ☐_____

Appendix C
Approved subcontractors

#1 Subcontractor	Hetzner Online data center (ISO/IEC 27001 certified)	
Subject of the order	Data types and categories	Circle of those affected
On-site support with administration (helping hands), server hosting, support	Access to basic infrastructure and encrypted content.	No direct access to application or database data.

# 2 Subcontractor	LogMeIn Ireland Ltd, Bloodstone Building Block C, 70 Sir John Rogerson's Quay, Dublin 2, Ireland	
Subject of the order	Data types and categories	Circle of those affected
Support software for conducting online meetings	Screen contents	Employees of the client

#3 Subcontractor	Markos Tafakis (external service provider) based in Nuremberg	
Subject of the order	Data types and categories	Circle of those affected
Sales and consulting	According to Annex B	According to Annex B

#4 Subcontractor	TeamViewer GmbH, Jahnstr. 30, 73037 Göppingen	
Subject of the order	Data types and categories	Circle of those affected
Support software for conducting online meetings	Screen contents	Employees of the client

#5 Subcontractor	Amazon Web Services Inc, 410 Terry Ave North, Seattle, WA 98109- 5210, US		Third country transfer on the basis of an adequacy decision (Data Privacy Framework)
Subject of the order	Data types and categories	Circle of those affected	
On-site support with administration (helping hands), server hosting, support	Access to basic infrastructure and encrypted content.	No direct access to application or database data.	

#6 Subcontractor	Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18		Third country transfer on the basis of an adequacy decision (Data Privacy Framework)
Subject of the order	Data types and categories	Circle of those affected	
Microsoft 365 Azure	According to Annex B	According to Annex B	

#7 Subcontractor	Cloudflare Germany GmbH, Rosental 7, c/o Mindspace, 80331 Munich, Germany		Third country transfer on the basis of an adequacy decision (Data Privacy Framework)
Subject of the order	Data types and categories	Circle of those affected	
DNS and CDN services	IP address	Users of the system	

Shared responsibility

#1 Jointly responsible persons	PayPal Braintree, Chicago, Illinois, United States	
Subject of the order	Data types and categories	Circle of those affected
Payment service provider, integrated in online platform	Last name, first name, e-mail address, company affiliation, payment information	Main contact person for customers (paying account)

#2 Jointly responsible parties	CardinalCommerce, 8100 Tyler Blvd Mentor, OH 44060	
Subject of the order	Data types and categories	Circle of those affected
Payment service provider for VISA	Last name, first name, e-mail address, company affiliation, payment information	Main contact person for customers (paying account)

Appendix D
Technical and organizational measures (TOM) in accordance with Art. 32 GDPR

1 Objective

It is the intention and duty of the management of Ingentis Softwareentwicklung GmbH to comply with all legal regulations relating to data protection and to protect the personal rights of every individual. This applies to every applicant and employee as well as customers, suppliers, and business partners. Furthermore, the aim of the company management is to protect the company's data. All employees of Ingentis Softwareentwicklung GmbH are bound by guidelines to these objectives. The managers ensure compliance with these guidelines in their area. The information security measures are based on the requirements of Art. 32 GDPR.

2 IT security guidelines

There is a comprehensive, binding set of rules for handling data and IT systems. The following points, among others, are regulated separately here:

- Network infrastructure (internal, external, LAN, WAN, WLAN)
- Password policy
- Authorization management
- E-mail and Internet use
- Use of software
- Handling company and customer data
- External access to the LAN
- ...

Every employee is obliged in writing to comply with the IT security guidelines.

3 Data protection officer

For Ingentis Softwareentwicklung GmbH is

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

has been appointed in writing as an external data protection officer (eDSB). The data protection officer performs all tasks incumbent upon him/her in accordance with the GDPR.

3.1 Commitment

All employees of Ingentis Softwareentwicklung GmbH are bound by an obligation of confidentiality in accordance with Art. 28 para. 3 lit. b, Art. 39 para. 1 lit. a GDPR and § 88 TKG (telecommunications secrecy) when they are hired.

Employees are made aware of and trained in the requirements of data protection through instructions and information.

3.2 Contract data processing in accordance with Art. 28 GDPR

After commissioning, Ingentis Softwareentwicklung GmbH processes, collects, or uses personal data on behalf of the customer within the meaning of Art. 28 GDPR. The object of the contractual relationship comprises the processing of personal data in accordance with the main contract concluded. The agreement on commissioned processing in accordance with Art. 28 GDPR regulates the protection of personal data in the case of commissioned data processing.

Ingentis Softwareentwicklung GmbH shall support the Customer in complying with its obligations under data protection law, in particular regarding notification, provision of information, correction, blocking and deletion within the scope of its possibilities.

If subcontractors need to be commissioned, the same data protection obligations will be imposed as are set out in customer DP contracts. It is ensured that the appropriate technical and organizational measures are implemented by the subcontractor in such a way that the processing is carried out in accordance with the requirements of data protection law.

3.3 Data protection documentation

The following data protection documents were created by me and updated as required:

- List of processing activities (Art. 30 GDPR)
- The technical and organizational measures pursuant to Art. 32 GDPR

4 Technical and organizational measures (Art. 32 GDPR)

1 Confidentiality (Art. 32 para. 1 lit. b GDPR)

Access control No unauthorized access to data processing systems,	Measures to prevent unauthorized persons from gaining access to data processing systems with which the personal data is processed and used: • *Key with key handover protocol* Employees can be identified by a unique number on the key. Logging takes place automatically when a key is issued using the programming software provided for this purpose. • *Security locking cylinder* The doors are equipped with a security locking cylinder with programmable chip keys. • *Server room locking system* Server rooms are equipped with an electronic locking system, keys are only accessible to a very restricted group of people. • Visitors are received in the entrance area and are not granted access to IT systems. • Video surveillance in outdoor areas.
Access control No unauthorized reading, copying, modification or removal within the system	Measures that ensure that persons authorized to use a data processing system can only access the data subject to their access authorization and that personal data cannot be read, copied, modified, or removed without authorization during processing, use and after storage: The data that we receive to verify problems or errors in our applications is stored in special directories to which only authorized employees have access. Once the problem has been resolved, this data is automatically deleted. In general, an authorization concept is in place to ensure that each employee only has access to the data required for their project. The authorizations can be changed at any time by system administrators. External access is secured on the data side by firewall systems. External data connections are protected using VPN technology.
Separation control Separate processing of data collected for different purposes	Measures to ensure that data collected for different purposes can be processed separately: Client-controlled applications

	Client-controlled applications with earmarking mechanisms
Pseudonymization The processing of personal data in such a manner that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures. (Art. 32 para. 1 lit. a GDPR; Art. 25 para. 1 GDPR)	As far as possible, pseudonymized personal data is used.

2 Integrity (Art. 32 para. 1 lit. b GDPR)

Transfer control No unauthorized reading, copying, modification or removal during electronic transmission or transport	Measures to ensure that personal data cannot be read, copied, altered, or removed by unauthorized persons during electronic transmission or during transport or storage on data carriers and that it is possible to verify and establish to which bodies personal data are intended to be transmitted by data transmission equipment: Personal data is only passed on in agreement with the owner (e.g. customer) of the data. In this case, the data is only passed on as agreed with the owner. In general, it is possible to transfer data in encrypted form and secure it accordingly via VPN connections.
Input control Determining whether and by whom personal data has been entered, modified, or removed from data processing systems	Measures that ensure that it is possible to subsequently check and determine whether and by whom personal data has been entered, modified, or removed from data processing systems: Events are logged on special systems (operating system level, firewall and VPN dial-in).

3 Availability and resilience (Art. 32 para. 1 lit. b GDPR)

Availability control	Systems with RAID Local emergency power supply (UPS) Backup system (the backup tapes are stored securely outside the company) Firewall Virus protection Regular patching of operating systems and applications
Rapid recoverability (Art. 32 para. 1 lit. c GDPR)	The recoverability of backup data is tested by means of restore checks.

4 Procedures for regular review, assessment and evaluation
(Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

Incident response management	A special reporting process has been modeled and implemented that informs those affected and the supervisory authority in the event of a security incident.
Data protection-friendly default settings (Article 25 (2) GDPR)	The principles of "privacy by design" and "privacy by default" are considered in IT operations and IT development.
Order control	There is no data processing within the meaning of Art. 28 GDPR without corresponding instructions from the client, e.g: Clear contract design, formalized order management, strict selection of the service provider, obligation to convince in advance, follow-up checks.