

Data Processing Agreement pursuant to Article 28 GDPR

between

Business customers of the “FASTCUBE Fixture Builder” platform

as Controller

— hereinafter referred to as the “Controller” —

and

CENIT AG

Industriestraße 52-54
70565 Stuttgart
Germany

as Processor

— hereinafter referred to as the “Processor” —

The Controller and the Processor are each also referred to as a “**Party**” and together as the “**Parties**”.

Preamble

The Controller has commissioned the Processor to provide the services specified in Section 1. Performance of the agreement involves the processing of personal data for which the Controller is the controller within the meaning of Article 4(7) GDPR. This Data Processing Agreement specifies the Parties’ data protection rights and obligations pursuant to Article 28(3) of the General Data Protection Regulation (GDPR) in connection with the handling by the Processor or third parties engaged by it as sub-processors of the Controller’s personal data for the performance of the Main Agreement.

The definitions set out in the GDPR shall apply.

Table of Contents

1.	Subject Matter and Term of the Agreement	2
2.	Description of the Processing	2
3.	Right to Issue Instructions	3
4.	Obligations of the Processor	3
5.	Technical and Organisational Security Measures	5
6.	Controller's Audit Rights	5
7.	Engagement of Sub-processors	5
8.	International Data Transfers	6
9.	Erasure of Controller Data	8
10.	Liability	8
11.	Final Provisions	8

1. Subject Matter and Term of the Agreement

- 1.1 The Processor shall provide the Controller with the following services on the basis of the agreement (the "Main Agreement") in connection with the provision of cloud/SaaS services, in particular the provision of browser-based SaaS applications for automated fixture design.

In this context, the Processor shall have access to personal data and shall process such data exclusively on behalf of and in accordance with the Controller's instructions, unless the Processor is required to carry out other processing by Union or Member State law to which it is subject. The Controller shall be solely responsible for assessing the lawfulness of the data processing pursuant to Article 6(1) GDPR.

- 1.2 The Parties enter into this Agreement to specify their respective rights and obligations under data protection law. In the event of doubt, the provisions of this Agreement shall prevail over the provisions of the Main Agreement.
- 1.3 The provisions of this Agreement shall apply to all activities connected with the Main Agreement in the course of which the Processor and its employees or persons engaged by the Processor come into contact with personal data originating from the Controller, collected for the Controller or otherwise processed on its behalf (hereinafter "Controller Data").
- 1.4 The Processor shall process the data only for the period specified in Annex 1.

2. Description of the Processing

Details of the processing operations, in particular the categories of personal data, the categories of data subjects and the purposes for which the personal data are processed on behalf of the Controller, are set out in Annex 1. In all other respects, the scope and purpose of the data processing by the Processor are governed by the Main Agreement (and, where available, the related service description).

3. Right to Issue Instructions

- 3.1 The Processor may collect, use or otherwise process Controller Data only within the scope of the Main Agreement and in accordance with the Controller's instructions; this applies in particular to transfers of personal data to a third country or an international organisation. If the Processor is required to carry out further processing by European Union or Member State law to which it is subject, it shall inform the Controller of that legal requirement before processing. The Processor may refrain from providing such information only to the extent and for as long as the law concerned expressly prohibits such information on important grounds of public interest.
- 3.2 The Controller's instructions are initially laid down in the Main Agreement and this Agreement and may subsequently be amended, supplemented or replaced by documented instructions issued by the Controller in writing or in a documented electronic format (each a "Documented Instruction"). The Controller is entitled to issue data protection instructions at any time insofar as the Processor's processing of Controller Data is concerned. This includes, in particular, instructions regarding the rectification, erasure and restriction of Controller Data and regarding the technical and organisational measures adopted by the Processor in connection with the processing of Controller Data.
- 3.3 The Controller shall document all instructions issued and retain them for the duration of their validity and for three further full calendar years thereafter. Instructions that go beyond the services agreed in the Main Agreement shall be treated as a request for a change in services.
- 3.4 If the Processor considers that an instruction from the Controller infringes data protection law, it shall notify the Controller without undue delay. The Processor is entitled to suspend implementation of the instruction concerned until it is confirmed or amended by the Controller. The Processor may refuse to implement an instruction that is manifestly unlawful.

4. Obligations of the Processor

- 4.1 The Processor shall comply with the statutory provisions on data protection. Documents and data shall be secured against access by unauthorised persons, taking into account the state of the art.
- 4.2 The Processor has appointed the following company data protection officer:

intersoft consulting services AG

Beim Strohhaus 17

20097 Hamburg

Tel.: +49 711 7825-30

Fax: +49 711 7825-4000

Email: datenschutzbeauftragter@cenit.com

- 4.3 The Processor shall bind all persons whom it entrusts with handling and performing this Agreement (hereinafter “Engaged Persons”) to confidentiality, unless they are already subject to an appropriate statutory duty of confidentiality (confidentiality obligation, Article 28(3)(b) GDPR), instruct them regarding the specific data protection obligations arising from this Agreement and the applicable limitation to instructions and purposes, and exercise due care to ensure compliance with those obligations.
- 4.4 Taking into account the nature of the processing, the Processor shall, insofar as possible, assist the Controller through appropriate technical and organisational measures in fulfilling requests to exercise the rights of data subjects laid down in Chapter III GDPR. If a data subject contacts the Processor directly in order to exercise rights relating to Controller Data processed on behalf of the Controller, the Processor shall forward that request to the Controller without undue delay. The Controller shall reimburse the Processor for the resulting expenditure if and to the extent permitted under applicable data protection law.
- 4.5 Taking into account the nature of the processing and the information available to the Processor, the Processor shall assist the Controller through appropriate technical and organisational measures in complying with the obligations laid down in Articles 32 to 36 GDPR, in particular with regard to security of processing, notification of personal data breaches, data protection impact assessments and consultation with supervisory authorities. The Controller shall reimburse the Processor for the resulting expenditure if and to the extent permitted under applicable data protection law.
- 4.6 In the event of disruptions, suspected data protection breaches or breaches of the Processor’s contractual obligations, suspected security incidents or other irregularities in the processing of Controller Data by the Processor, by Engaged Persons involved in performing the engagement or by third parties, the Processor shall inform the Controller within a reasonable period. The same applies to inspections of the Processor by the data protection supervisory authority. To the extent possible, notice of a personal data breach affecting Controller Data shall include the following information:
- a) a description of the nature of the personal data breach, where possible including the categories and number of data subjects concerned and the categories and number of personal data records concerned;
 - b) a description of the likely consequences of the breach; and
 - c) a description of the measures taken or proposed by the Processor to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

The Processor shall take the necessary measures without undue delay to secure the data and mitigate possible adverse effects on the data subject(s), inform the Controller thereof and request further instructions. In addition, the Processor shall provide the Controller with information at any time insofar as its Controller Data are affected by a breach within the meaning of the first sentence.

- 4.7 The Processor shall provide the Controller with the information required to maintain the record of processing activities.

5. Technical and Organisational Security Measures

Within its area of responsibility, the Processor shall structure its internal organisation so as to meet the specific requirements of data protection and shall ensure that it has implemented all necessary technical and organisational measures for the appropriate protection of the Controller's data pursuant to Article 32 GDPR, including at least the security measures set out in Annex 2. If special categories of personal data are also processed, the Processor shall additionally implement the appropriate and specific measures resulting from Section 22(2) of the German Federal Data Protection Act (BDSG). The Processor reserves the right to amend the security measures implemented, provided that it ensures that the contractually agreed level of protection is not reduced. The Controller may request an up-to-date version of the technical and organisational security measures implemented by the Processor at any time. The Processor shall inform the Controller in text form of any material changes to the security measures.

6. Controller's Audit Rights

- 6.1 Before processing commences and regularly thereafter, the Controller shall satisfy itself that the Processor complies with the obligations laid down in this Agreement, in particular the technical and organisational measures. At the Controller's request, the Processor shall also permit audits of the processing activities covered by these clauses at reasonable intervals or where there are indications of non-compliance and shall contribute to such audits. When deciding on a review or audit, the Controller may take into account relevant certifications held by the Processor.
- 6.2 The Controller may conduct the audit itself or appoint an independent auditor. Audits may also include inspections at the Processor's premises or physical facilities and shall, where appropriate, be carried out with reasonable prior notice, unless this would jeopardise the purpose of the review. The Controller shall conduct audits only to the extent necessary and shall not disproportionately disrupt the Processor's business operations.
- 6.3 The Processor undertakes, upon the Controller's oral, written or electronic request, to make available within a reasonable period all information and evidence required to audit compliance with the obligations laid down in this Agreement and with the Processor's technical and organisational measures, and to permit on-site inspections.
- 6.4 The Controller shall bear all costs of audits unless an audit reveals a material breach of this Agreement by the Processor; in that case, the Processor shall bear its own costs of the audit. If an audit shows that the Processor has failed to comply with its obligations under this Agreement, the Processor shall remedy the breach within a reasonable period at its own expense.

7. Engagement of Sub-processors

- 7.1 The Processor has the Controller's general authorisation to engage the Sub-processors listed in Annex 3 to this Agreement. The Processor shall expressly inform the Controller

in writing at least four (4) weeks in advance of any intended changes to that list through the addition or replacement of Sub-processors, thereby giving the Controller sufficient time to object to such changes before the relevant Sub-processor(s) are engaged. The Processor shall provide the Controller with the information necessary to exercise its right to object. If the Controller does not object within the four (4)-week period, the new Sub-processor shall be deemed accepted by the Controller.

- 7.2 If the Controller has legitimate grounds under data protection law to object to the processing of personal data by the new Sub-processor(s), the Controller may terminate the Agreement, limited to the service for which the new Sub-processor is to be engaged, by written notice to the Processor. Such termination shall take effect on the date specified by the Controller, but no later than when the new Sub-processor assumes performance of the services.
- 7.3 Where the Processor engages a Sub-processor to carry out specific processing activities on behalf of the Controller, such engagement must be governed by a subcontract imposing on the Sub-processor the same data protection obligations as those applicable to the Processor under this Agreement. The Processor shall ensure that the Sub-processor complies with the obligations to which the Processor is subject under these clauses and the GDPR. The Processor shall ensure that the Controller may exercise its rights under this Agreement, in particular its review and audit rights, directly against the Sub-processors as well. The Processor shall carefully select Sub-processors on the basis of their suitability and reliability.
- 7.4 Any further subcontracting by the Sub-processor requires the Controller's express consent.
- 7.5 Sub-processing within the meaning of these provisions does not occur where the Processor commissions third parties to provide services that are to be regarded as purely ancillary. These include, for example, postal, transport and shipping services, cleaning services, telecommunications services with no specific connection to the services provided by the Processor to the Controller, and security services. Maintenance and inspection services constitute subcontracting arrangements subject to this Section 7 insofar as they are provided for IT systems that are also used in connection with the provision of services to the Controller.

8. International Data Transfers

- 8.1 The Processor shall not transfer Controller Data processed under this Agreement to, or have such data processed in, a country outside the European Union or the European Economic Area (EEA) for which no adequacy decision of the European Commission pursuant to Article 45(3) GDPR exists (a "Non-Adequate Third Country"), unless such transfer is permitted in accordance with Articles 44 et seq. GDPR.-
- 8.2 If the Processor is required under European Union or Member State law to which it is subject to transfer Controller Data to a Non-Adequate Third Country, the Processor shall inform the Controller of that legal requirement before carrying out the transfer,

unless the law concerned prohibits such notification on important grounds of public interest.

8.3 A transfer of Controller Data to a Non-Adequate Third Country is permitted in particular where an appropriate safeguard within the meaning of Article 46 GDPR is in place, in particular through:

a) execution of the then-current standard contractual clauses of the European Commission (SCCs) pursuant to Article 46(2)(c) GDPR;

b) binding corporate rules (BCRs) pursuant to Article 47 GDPR; or

c) another permissible transfer mechanism pursuant to Article 46 GDPR.

8.4 Where standard contractual clauses or binding corporate rules are used, the Processor shall ensure that

- an assessment of the legal framework and practices in the third country (transfer impact assessment) is carried out before the transfer; and
- where appropriate, supplementary technical and organisational measures are implemented to ensure a level of protection essentially equivalent to that guaranteed by the GDPR.

8.5 The engagement of Sub-processors in a Non-Adequate Third Country is permitted only if

- the relevant Sub-processor has been duly authorised in accordance with this Agreement;
- the requirements of Article 28(2) and (4) GDPR are met; and
- the requirements of Articles 44 et seq. GDPR are complied with, in particular through appropriate contractual safeguards.

9. Erasure of Controller Data

- 9.1 Upon completion of the processing services covered by the Agreement or expiry of the term of this Agreement, the Processor shall, at the Controller's option, either erase all personal data provided to it or return such data to the Controller, unless and to the extent that European Union law or the law of the Federal Republic of Germany requires further storage of the personal data.
- 9.2 The foregoing obligation also extends to any backups held by the Processor. Statutory retention obligations remain unaffected; for their duration, the data concerned shall be blocked from further processing and processed exclusively for the purposes prescribed by law.
- 9.3 At the Controller's request, the Processor shall provide appropriate evidence that the data have been erased or returned in accordance with the Agreement.

10. Liability

Reference is made to Article 82 GDPR. In all other respects, the limitations of liability set out in the Main Agreement shall apply.

11. Final Provisions

- 11.1 The Parties agree that the Processor shall be precluded from asserting a right of retention within the meaning of Section 273 of the German Civil Code (BGB) with respect to the data to be processed and the associated data carriers.
- 11.2 Amendments and supplements to this Agreement must be made at least in written form or in a documented electronic format.
- 11.3 Should any provision of this Agreement be or become wholly or partly legally invalid or unenforceable, the validity of the remaining provisions shall not be affected.
- 11.4 This Agreement shall be governed by German law. The courts at the Processor's registered office shall have exclusive jurisdiction.

The following documents form an integral part of this Agreement:

Annex 1: Description of the Processing

Annex 2: Technical and Organisational Measures of the Processor for Data Protection pursuant to Article 32 GDPR

Annex 3: Sub-processing Arrangements of the Processor

Controller

(Place/Date)

(Signature)

Processor

(Place/Date)

(Signature)

Annex 1:

Description of the Processing

I. Categories of Data Subjects Whose Personal Data Are Processed

- | | |
|--|---|
| ☒ Prospective Customers | Visitors to the platform, prospective registrants, companies undergoing the verification process |
| ☒ Customers | Business customers of the FASTCUBE platform, users (Member, Admin, Owner) with or without an active subscription, employees and other users of business customers |
| ☒ Users | Users of the FASTCUBE platform, users of the customer portal, persons making support enquiries |

II. Categories of Personal Data Processed

- | | |
|--|--|
| ☒ Personal Master Data | First and last name, company affiliation, user role (e.g. Owner, Member, Maker, Viewer) |
| ☒ Address Data | Company address, country, town/city, postal code |
| ☒ Contact Data | Business email address, telephone number, contact-person details |
| ☒ Payment/Banking Data | Billing address, VAT identification number, payment and transaction data, order and subscription information, payment information processed by Stripe |
| ☒ Technical Data | IP address, login and authentication data, in particular user identifier, Microsoft Entra ID information, OTP information, log files, in particular database queries, timestamps and login actions, CAD data provided by the user and project data |
| ☒ Log Files, Device Information (Browser to Web Server) | Requested URL (specific page), access status/HTTP status code, volume of data transferred, website |

from which the request originates
(referrer URL), browser type,
browser language setting

☒ **Support and Communication Data**

Contents of support requests, ticket
information, email communications,
documentation of support and
remote-maintenance activities; data
that may be viewed or processed in
connection with remote-
maintenance or support services
(e.g. TeamViewer)

III. Nature of the Processing

Collection, recording, storage, retrieval, consultation, use, disclosure by transmission (to the Sub-processors Microsoft Azure and Stripe), restriction, erasure and destruction of personal data in connection with the provision and operation of the “FASTCUBE Fixture Builder” SaaS platform, including user registration, authentication, user administration, subscription management and technical platform operation.

IV. Purpose(s) for Which the Personal Data Are Processed on Behalf of the Controller

The processing is carried out for the purpose of providing, operating and administering the “FASTCUBE Fixture Builder” SaaS platform for the Controller and its authorised users. This includes in particular:

- Registration and administration of company accounts and user accounts
- Authentication and authorisation of users
- Provision of platform functionalities (project creation, fixture creation, data export)
- Administration of subscriptions and licence assignments
- Technical operation, error analysis and ensuring IT security
- Communication with users (system notifications, support requests)

V. Duration of the Processing

The term of this Agreement shall correspond to the term of the Main Agreement.

Annex 2:

Technical and Organisational Measures of the Processor for Data Protection pursuant to Article 32 GDPR

The technical and organisational measures implemented by the Processor, taking into account the nature, scope, context and purposes of the processing as well as the varying likelihood and severity of the risk to the rights and freedoms of data subjects, are described below.

1. Confidentiality pursuant to Article 32(1)(b) GDPR

1.1. Physical Access Control

The Processor shall implement measures designed to prevent unauthorised persons from gaining physical access to data processing facilities in which personal data are processed or used.

Data Centres (Processing of Controller Data)

The Processor does not operate its own data centres for the provision of the services covered by the Agreement. Processing takes place in data centres of Microsoft Ireland Operations Ltd. in the “Germany West Central” Azure region (Frankfurt am Main, Germany). Physical access is secured there by the following measures implemented by the Sub-processor:

- Multi-level physical access control system with perimeter security, access control barriers and personalised access credentials
- Biometric authentication in security-sensitive zones
- Security personnel on duty around the clock and video surveillance of access points and outdoor areas
- Access only following documented approval and on a need-to-know basis, subject to time limits and role-based restrictions
- Logging of all access, including escorting of visitors
- Evidence of certification to ISO/IEC 27001, ISO/IEC 27017 and ISO/IEC 27018, as well as SOC 1 and SOC 2 Type II audit reports

The Processor verifies the effectiveness of these measures on the basis of the certificates and audit reports provided by the Sub-processor and shall make them available to the Controller upon request.

Processor Sites (Administration and Support)

- Access to company premises and office areas only by means of personalised access cards whose use is electronically logged
- Staffed reception during business hours; visitors are registered and escorted
- Technical rooms and network rooms are separately locked and accessible only to a designated group of persons
- Documented process for issuing, blocking and returning access credentials when employees join or leave the company

- Mandatory clean-desk and clear-screen policy
- Destruction of physical data carriers and documents in compliance with data protection requirements and DIN 66399

1.2. System Access Control

Measures that prevent unauthorised persons from using data processing systems (computers).

Access to the Platform by the Controller's Users

- Authentication exclusively via Microsoft Entra ID; identity and authentication data are processed in the "Europe" Azure geolocation
- Users with their own Entra ID tenant authenticate through federation, so that the Controller's access policies, including multi-factor authentication and Conditional Access, apply directly.
- Users without a Microsoft account authenticate using a time-limited one-time password (OTP) sent to their business email address; no static password is issued for this method
- Each user account is assigned to an individual; shared or functional accounts for end users are not provided for
- Automatic account lockout after a defined number of unsuccessful login attempts and automatic termination of inactive sessions
- Login events, failed login attempts and security-relevant account changes are logged
- User accounts are created, amended and deactivated by the Controller's users holding the "Owner" or "Admin" role; the Controller is responsible for promptly revoking access when a user leaves

Access to Systems by the Processor's Employees

- Administrative access is performed exclusively through personalised administrative accounts that are separate from standard accounts and are subject to mandatory multi-factor authentication
- Access to the production environment only from managed company devices over encrypted connections; access from the open internet without prior authentication is technically prevented.
- Centrally enforced password policy specifying minimum length, complexity and blocking of compromised passwords
- End-user devices with full-disk encryption, centrally managed endpoint protection and automated patch management
- Documented onboarding and offboarding process; access is blocked without undue delay when an employee leaves
- Network segmentation and filtering by firewalls and Network Security Groups; database and backend services are not publicly accessible
- All transmissions are encrypted in transit exclusively using a current version of TLS

1.3. Data Access Control

Measures that ensure that persons authorised to use a data processing system can access only the data covered by their access authorisation and that personal data cannot be read, copied, altered or removed without authorisation during processing or use or after storage.

Authorisation Concept within the Platform

- Each Controller's data are assigned to a segregated workspace (company tenant). Access to other Controllers' data is technically prevented; each request is checked server-side against the authenticated user's tenant membership
- Within the company account, a role-based authorisation concept using the "Owner", "Admin" and "Member" roles provides graduated administrative permissions
- A user's functional scope is additionally limited by the assigned licence type ("Maker", "Viewer")
- Roles and licence types are granted and revoked by the Controller itself through the platform's user administration

Authorisations of the Processor's Employees

- Access rights are granted on a need-to-know and least-privilege basis and are linked to the respective role
- During normal operations, the Processor's employees do not access the Controller's content data. Such access occurs only as required for troubleshooting or at the Controller's request, is limited to the necessary extent and is logged
- Remote access for support purposes using TeamViewer or comparable tools takes place only with the Controller's prior consent and under its observation
- Access rights are requested, approved and revoked through a documented procedure; the authorisations of privileged accounts are reviewed at least annually
- Administrative activities in the production environment are logged; the logs are protected against alteration by the persons whose activities are logged
- All Engaged Persons are bound to confidentiality and have received data protection training

Protection of Stored Data

- All stored personal data are encrypted at rest using AES-256. This includes, in particular, databases, object storage and persistent storage volumes of the Kubernetes platform operated in Microsoft Azure. Encryption is implemented at the level of the Azure storage and database services.
- Cryptographic keys are managed through Azure Key Vault using a role-based authorisation concept.
- Separation of production, staging and development environments.
- Destruction of data carriers in the Sub-processor's data centres in accordance with NIST SP 800-88

1.4. Data Separation Control

Measures that ensure that data collected for different purposes are processed separately.

Separation between Controllers (Tenant Segregation)

- All projects, user accounts and work products are logically assigned to a company tenant. The tenant identifier is a mandatory component of every data record
- For each request, the assignment is checked server-side against the authenticated user's tenant membership. The check is performed in the application logic rather than in the user interface, thereby preventing circumvention through direct interface calls
- Object storage for workpiece models and export files is maintained in separate paths for each tenant, with separate access policies
- The effectiveness of tenant segregation is verified by automated tests whenever data-access paths are changed

Separation by Processing Purpose

- Identity and authentication data are processed in Microsoft Entra ID exclusively for authentication and to determine whether the user has been assigned a Maker licence.
- Payment and billing data are processed by the Sub-processor Stripe Payments Europe Ltd. The platform itself does not store complete payment data, but only reference identifiers.
- Technical log and operational data are stored separately from application data, with a separate authorisation concept and separate retention period
- Production, test and development environments are operated in complete separation. Production data are not transferred to test or development environments

1.5. Pseudonymisation (Article 32(1)(a) GDPR; Article 25(1) GDPR)

The processing covered by the Agreement requires users to be identifiable, since authentication, role assignment, licence assignment and attribution of project changes must be performed on a personal basis. Complete pseudonymisation of production operations is therefore not possible. The Processor implements the following measures:

- Analyses of product usage, error frequency and capacity planning are performed exclusively on aggregated or pseudonymised datasets that do not permit conclusions to be drawn about individual users
- Only synthetic or anonymised datasets are used in test and development environments
- In internal analyses, personal identifiers are replaced with technical identifiers that do not contain names; the mapping table is subject to a separate authorisation concept
- When log data are disclosed to third parties for error analysis, personal attributes are removed or replaced before transmission

2. Integrity (Article 32(1)(b) GDPR)

2.1. Disclosure Control

Measures that ensure that personal data cannot be read, copied, altered or removed without authorisation during electronic transmission or while being transported or stored on data carriers, and that it is possible to review and establish the entities to which personal data are intended to be transmitted using data transmission facilities.

Protection during Transmission

- All connections between the user's browser and the platform use exclusively a current version of TLS. Unencrypted connections are rejected server-side and redirected to the encrypted version
- HTTP Strict Transport Security is enabled; obsolete protocol versions and weak cipher suites are disabled
- Communication between the platform's services takes place within a closed network in Microsoft Azure that is not publicly accessible. Connections to database and storage services are likewise encrypted in transit
- Administrative access takes place exclusively over encrypted connections from managed company devices

Documentation of Transmission Routes

- All intended recipients of personal data are exhaustively documented in Annex 3 to this Agreement. No transmission takes place to any recipients other than those listed
- The purpose, scope and place of performance are documented for each recipient; changes are subject to the procedure set out in Section 7 of this Agreement
- The Controller's export of work products (.DXF, .STEP) takes place over the application's encrypted connection and is logged
- No transfer is made to third countries that are not covered by an adequacy decision

2.2. Input Control

Measures that ensure that it is subsequently possible to review and establish whether, and by whom, personal data have been entered into, altered in or removed from data processing systems.

- Every action on the platform is performed under a user identifier assigned to an individual. Processing performed anonymously or under shared accounts is not provided for
- The creation, amendment and erasure of user accounts, assignment and revocation of roles, and assignment and revocation of licence types are logged with a timestamp, the initiating user and the type of change
- Logins, failed login attempts and changes to authentication attributes are logged in Microsoft Entra ID
- Changes to projects and fixtures are attributed to the user account performing the work and stored with the time of the change
- Administrative interventions in the production environment by the Processor's employees are logged separately
- Log data are stored write-protected in a separate storage area. The persons whose activities are logged are not authorised to alter or erase the log entries relating to them
- The retention period for log data is defined; the data are automatically erased upon expiry

3. Availability and Resilience (Article 32(1)(b) GDPR)

3.1. Availability Control

Measures that ensure that personal data are protected against accidental destruction or loss.

- Operation in Microsoft Azure, “Germany West Central” region, with storage and database services redundantly deployed across several physically separate sites within the region
- Redundant design of the data-centre infrastructure by the Sub-processor, including uninterruptible power supply, emergency generators, redundant air conditioning, early fire detection and fire suppression systems
- Operation of the application in a container orchestration environment with automatic restart and redistribution of failed instances
- Regular automated backups of database and object-storage data; backups are encrypted and stored separately from production data
- Continuous monitoring of availability, utilisation and error rates, with automated alerts sent to a defined on-call group
- Protection against overload through upstream filtering, rate limiting and safeguards against distributed denial-of-service attacks
- Centrally managed malware detection on all end-user devices and automated patch and vulnerability management for platform components
- The contractually agreed availability of the platform is governed by the service description for the Main Agreement

3.2. Ability to Restore Availability (Article 32(1)(c) GDPR)

Measures that ensure the timely restoration of data availability following temporary loss of or damage to the data.

- Documented backup and restoration concept with defined targets for the maximum tolerable data loss (Recovery Point Objective) and maximum tolerable downtime (Recovery Time Objective)
- Point-in-time restoration of database data within the defined backup retention period
- Regular verification of recoverability through test restorations; the results are documented
- Fully automated, version-controlled deployment of the application environment, enabling the operating environment to be rebuilt reproducibly
- Documented emergency plan with defined roles, escalation paths and contact details
- The Controller remains responsible for maintaining adequate backups of its own application data; the Processor’s backups serve to restore system operations and do not replace backups by the Controller

4. Process for Regular Testing, Assessment and Evaluation (Article 32(1)(d) GDPR; Article 25(1) GDPR)

4.1. Data Protection Management

- Appointment of an external company data protection officer (intersoft consulting services AG, Hamburg), who can be contacted at datenschutzbeauftragter@cenit.com

- Maintenance of a record of processing activities pursuant to Article 30 GDPR
- Binding internal data protection policies; all Engaged Persons are bound to confidentiality pursuant to Article 28(3)(b) GDPR
- Regular training and awareness-raising for Engaged Persons on data protection and information security, at least annually
- Data protection review of new or modified processing activities before their introduction, including an assessment of whether a data protection impact assessment is required pursuant to Article 35 GDPR
- Documented procedure for selecting, reviewing and monitoring Sub-processors, including evaluation of submitted certificates and audit reports
- Regular review and updating of the measures described in this Annex, at least annually and additionally when material changes to the processing occur
- Documented procedure for handling data subject requests pursuant to Articles 15 to 22 GDPR, including assistance to the Controller pursuant to Section 4 of this Agreement

4.2. Incident Response Management

Measures for responding to security breaches.

- Documented process for detecting, reporting, assessing and handling security incidents and personal data breaches
- Central reporting point for security incidents; all Engaged Persons are required to report suspected incidents without undue delay
- Technical detection through continuous monitoring, alerts for security-relevant events and analysis of log data
- Defined roles, escalation levels and contact details for incident handling, including involvement of the data protection officer
- Assessment of each incident with regard to the notification obligation under Article 33 GDPR and the communication obligation under Article 34 GDPR
- Notification of the Controller without undue delay of personal data breaches affecting Controller Data, stating the nature of the breach, the categories of data affected, the likely consequences and the measures taken and proposed
- Documentation of all incidents, including root-cause analysis and resulting corrective measures
- The Processor shall assist the Controller in meeting its notification and communication obligations vis-à-vis the supervisory authority and the data subjects

4.3. Data Protection by Design and by Default (Article 25 GDPR)

- Data minimisation during registration: only data required for performance of the Agreement, authentication and operation are collected
- The Controller determines the scope of personal data processed on the platform. Processing of special categories of personal data pursuant to Article 9 GDPR is not envisaged
- By default, new users are assigned the “Member” role and the “Viewer” licence type, i.e. the lowest level of authorisation. Extended permissions must be actively assigned by the Controller

- The Processor's employees have no access to content data during normal operations; access occurs only when specifically required and is logged
- Remote-maintenance access for support purposes requires the Controller's prior consent
- Data protection requirements form an integral part of the development process; security-relevant changes are subject to review by a second person before deployment to the production environment
- Defined erasure periods: following erasure of the company account, all customer data are irretrievably erased after 30 calendar days unless statutory retention obligations prevent such erasure
- The Controller independently administers user accounts, roles and licence assignments and may revoke access itself at any time

4.4. Instruction Control

Measures that ensure that personal data processed on behalf of the Controller are processed only in accordance with the Controller's instructions.

- Written data processing agreement pursuant to Article 28 GDPR clearly specifying the subject matter, duration, nature, purpose and scope of the processing in Annex 1
- Binding all Engaged Persons to confidentiality and compliance with the limitation to instructions, and instructing them regarding the data protection obligations arising from this Agreement
- Documented procedure for receiving, reviewing and implementing the Controller's Documented Instructions; designated contacts authorised to issue and receive instructions
- Review of incoming instructions for compliance with data protection law; where an infringement is apparent, the Controller is notified without undue delay in accordance with Section 3 of this Agreement
- No processing for the Processor's own purposes; in particular, no use of Controller Data for the Processor's own analyses, advertising or model training
- Careful selection of Sub-processors on the basis of suitability and reliability; contractual flow-down of the same data protection obligations and limitation to instructions, documented in Annex 3
- Regular review of Sub-processors on the basis of certificates and audit reports submitted
- Enabling reviews and audits by the Controller pursuant to Section 6 of this Agreement, including provision of the required information and evidence
- At the Controller's request, evidence of the erasure or return of Controller Data in accordance with instructions following termination of the Agreement

Annex 3:

Sub-processing Arrangements of the Processor

Sub-processor (Company Name Including Legal Form)	Description of the (Partial) Services	Address/Place of Performance	Measures to Ensure an Adequate Level of Protection pursuant to Articles 44 et seq. GDPR
Stripe Payments Europe Limited	Payment processing	One Wilton Park, Wilton Place, Dublin 2, D02 FX04, Ireland	Transfers exclusively to countries covered by an adequacy decision, to companies certified under the Data Privacy Framework or using the EU Standard Contractual Clauses (SCCs).
Microsoft Ireland Operations Ltd.	Provision of cloud infrastructure (Azure) for operation, storage and authentication (Microsoft Entra ID)	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland; place of processing: “Germany West Central” Azure region (Frankfurt am Main, Germany), Entra ID: “Europe” Azure geolocation	Processing within the EU/EEA; no transfer to Non- Adequate Third Countries. Evidence: ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC 1 and SOC 2 Type II