Appendix 1 - Agreement on the processing of personal data

This Appendix is drawn up pursuant to Article 28.3 of the European Regulation 2016/679 from the European Parliament and Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("General Data Protection Regulation" or ("GDPR") (hereinafter the "**Regulation**").

It is an integral part of the CENIT KEONYS FR General Terms and Conditions of Sale (the "**Contract**").

Capitalised terms used in this Appendix shall have the meaning ascribed to them in the GDPR or in the Contract.

1.1. The Parties acknowledge that when CENIT KEONYS FR processes Personal Data on behalf of the CUSTOMER within the framework of the execution of the Contract, it acts as a Data Processor and the CUSTOMER acts as a Data Controller.

The personal data processed are identification data (surname, first name, professional email address, professional telephone number). The categories of data subjects concerned by the Processing are the Customer's employees or service providers.

Therefore, CENIT KEONYS FR undertakes to act in accordance with the documented instructions of the CUSTOMER (including for the transfer of Personal Data outside the EU).

The CUSTOMER's instructions for Processing Personal Data must be lawful and in accordance with the Regulation; the CUSTOMER is solely responsible for the accuracy, quality and lawfulness of the Personal Data and the means by which it has acquired the Personal Data.

1.2. If CENIT KEONYS FR considers that one of the CUSTOMER's instructions constitutes a violation of the GDPR or of any other provision of EU law or of the law of the Member States relating to data protection, it will inform the CUSTOMER as soon as possible, without this notice constituting a legal opinion or legal advice. CENIT KEONYS FR is entitled to suspend the execution of this instruction until the CUSTOMER confirms or modifies it.

1.3. CENIT KEONYS FR undertakes:

a) To guarantee the confidentiality of the Personal Data processed on behalf of the CUSTOMER;
b) Not to use the Personal Data collected as a Data Processor of the Customer for any other purpose than those set out in this Appendix except where expressly permitted by Article 28 (3)(a) of the GDPR;
c) To implement appropriate and reasonable technical measures to ensure the protection of Personal Data processed on behalf of the CUSTOMER. In particular, CENIT KEONYS FR undertakes to implement the following security measures:
    - Measures to ensure the confidentiality, integrity, availability and resilience of processing systems and services;
    - Measures to restore availability and access to personal data within an appropriate timeframe in the event of a physical or technical incident;
    - A procedure to regularly test, analyse and evaluate the effectiveness of technical and organisational measures to ensure the security of processing;

    The Customer acknowledges that these measures are likely to evolve due to future knowledge and technical developments. CENIT KEONYS FR is therefore expressly authorised to implement alternative measures to those described as long as these measures maintain the general level of security as described above.

d) To ensure that access to Personal Data is limited to those staff and sub-processors who need access to it for the provision of the services under the Contract;
e) To notify the CUSTOMER by e-mail or post as soon as possible after becoming aware of any breach of personal data, provide all relevant information, and take all reasonable steps to remedy the breach, of which it shall keep the CUSTOMER informed. The notification shall be accompanied by all relevant documentation to enable the CUSTOMER to notify the competent supervisory authority of the breach;
f) To assist the CUSTOMER, as far as possible, in the management of requests or claims made by the Data Subjects in the exercise of their rights. When the Data Subjects exercise their rights directly with CENIT KEONYS FR, the latter must address these requests as soon as they are received to the CUSTOMER's DPO by e-mail.
g) To cooperate with the competent data protection authorities.

1.4. The CUSTOMER authorises CENIT KEONYS FR to use one or more sub-processors for the Processing of Personal Data. In particular, the CUSTOMER authorises CENIT KEONYS FR to use the company CENIT AG (parent company) located at 54 Industrie Strasse - Stuttgart - Germany, which performs the security and backup of the Data hosted by CENIT KEONYS FR. The CUSTOMER agrees that CENIT AG may use the sub-processors listed in Schedule 3 for the performance of the Contract. CENIT KEONYS FR undertakes to inform the CUSTOMER in writing of any planned change concerning the addition or replacement of subsequent sub-processors by indicating the Contract reference. The CUSTOMER may object, for justified and legitimate reasons, to the use of a new sub-processor by notifying CENIT KEONYS FR by e-mail within ten (10) days from the receipt of the notification from CENIT KEONYS FR, under the conditions of article 28 paragraph 3 of the GDPR.

In any case, CENIT KEONYS FR will impose on its authorised data processors the same obligations to protect Personal Data as those set out in this Appendix. CENIT KEONYS FR will also ensure that its sub-processors do not process Personal Data for purposes other than those necessary to provide the subcontracted services.

1.5. Any transfer of Personal Data shall be implemented in accordance with the Regulation.

If CENIT KEONYS FR or one of the sub-processors processes or transfers Personal Data outside the European Union, in a country that does not have an adequate level of protection as defined by the European Commission, the CUSTOMER mandates CENIT KEONYS FR to sign in its name and on its behalf with the legal entities concerned a data transfer contract established on the basis of the European Commission's Standard Contractual Clauses for the transfer of Personal Data to companies established in third countries (the "Contractual Clauses for the Transfer of Data" or

"EUSCC"). Alternatively, transfers will be managed by means of a substitute mechanism validated and recognised by the European authorities as ensuring an adequate legal framework to secure the Processing of Personal Data outside the European Union.

CENIT KEONYS FR specifies that no transfer of Personal Data is made outside the EU.

1.6. The CUSTOMER may verify, at the most once a year, the respect by CENIT KEONYS FR of all the obligations resulting from the present agreement or may mandate an auditor of its choice for this purpose, as long as it is not a competitor of CENIT KEONYS FR.

Such audit shall be conducted (i) during CENIT KEONYS FR' normal business hours, (ii) without interfering with CENIT KEONYS FR' business operations, and (iii) with appropriate notice and after consultation with CENIT KEONYS FR.

The Customer shall bear its own expenses in connection with such audit and shall compensate CENIT KEONYS FR for the cost of its internal resources required to conduct the on-site audit (on the basis of time and materials according to the then current price list) if the audit does not reveal a serious breach by CENIT KEONYS FR of its obligations under this Appendix (in which case CENIT KEONYS FR shall promptly remedy the breach at its own expense).

1.7. CENIT KEONYS FR will respect the CUSTOMER's instructions concerning the retention of personal Data and, at the CUSTOMER's choice and request, undertakes to destroy or return to the CUSTOMER, within the period agreed with it, all the personal Data, including all copies which may have been made on any medium whatsoever, except in case of necessity of retention required by a law or regulation.

In any case, the Personal Data processed by CENIT KEONYS FR within the framework of the Contract will be kept for the duration of the Contract plus the duration of the applicable statute of limitations necessary for CENIT KEONYS FR to ensure the defence of its rights.

In case of deletion, CENIT KEONYS FR shall specify beforehand to the CUSTOMER the procedures for the deletion of the Personal Data.

1.8. CENIT KEONYS FR also specifies that it has appointed a Personal Data Protection Officer (DPO) whose contact details are given below: dataprotection@keonys.com

SCHEDULE 1 – DETAILS OF PERSONAL DATA PROCESSING

1. Integration and/or Migration Services

- Purpose of processing: purpose defined by the CUSTOMER as Data Controller
- Object of processing: performance of the services stipulated in the Contract signed by the Parties
- Nature of processing operations: collection, recording, structuring, interconnection, destruction
- Data subjects: CUSTOMER’s users
- Categories of personal data: data specified in the Contract
- Retention period: duration of the Contract

2. Training Services

- Purpose of processing: management of funding and coverage of professional training programs
- Object of processing: performance of the services stipulated in the Contract signed by the Parties
- Nature of processing operations: collection, recording, hosting, modification, disclosure, destruction
- Data subjects: CUSTOMER’s employees
- Categories of personal data: data specified in the Contract
- Retention period: duration of the Contract

3. Level 1 User Support Services

- Purpose of processing: management and monitoring of user support ; escalation of information to the software publisher for support purposes
- Object of processing: performance of the services stipulated in the Contract signed by the Parties or the publisher
- Nature of processing operations: Collection, recording, hosting, modification, disclosure, destruction
- Data subjects: CUSTOMER’s users
- Categories of personal data: data specified in the Contract
- Retention period: duration of the Contract

SCHEDULE 2 – SECURITY MEASURES

CENIT KEONYS FR takes all necessary precautions to ensure the security of the data processed, in particual regarding their confidentiality, integrity, and availability.

CENIT KEONYS FR hereby declares that it implements the following technical and organizational security measures.

Technical and organizational measures

1. Measures to ensure confidentiality

1.1 Access Intended to prevent unauthorized persons from gaining spatial access to data processing systems. Measures to secure buildings and rooms.	**Available**
Locking system	☒
Special glazing	☐
Careful selection of external security guards	☒
Surveillance	☒
Biometric access control	☐
Security service on site / security outside working hours	☒
Personal verification at the gatekeeper / reception	☒
Time-restricted access to public areas	☒
Authorization cards (through access chips with RFID)	☒
Visitor passes	☐
Logging of visitor access / visitor book	☒
Accompaniment of visitor access by our own employees	☒
Electronic access code cards/access transponders	☒
Key regulation	☒
Access authorization concept	☒

Tiered security areas and controlled access	☒
Secure entrance for arrivals and deliveries	☐
Separately secured access to the server room	☒
Separately secured access to the data center	☒
Work instructions/guidelines regarding locking premises when leaving/ending work	☒
Careful selection of cleaning staff	☒
Other measures: Click here to enter text.	☐

1.2 Physical access control To prevent unauthorized access to and use of data processing systems. System protection.	**Available**
Assignment of user rights according to the "need to know" principle	☒
Creating User Profiles	☒
Authorization management	☒
Documented process for assigning rights when new employees join the company	☒
Documented process for revocation of rights in the event of a change of department of employees	☒
Documented process for revocation of rights in the event of employee resignation	☒
Functional and/or time-limited assignment of user authorizations	☒
Use of individual passwords	☒
Login with username and password	☒
Automatic password-protected lock of the screen after inactivity (screensaver)	☒
Password policy with minimum password complexity requirements:	☒

• At least 12 characters	☒
• Upper and lower case, special characters, number (of which at least three criteria)	☒
• Prevention of trivial passwords (e.g. password1, password2, 123456, qwerty)	☒
• Password history (no reuse of the last 13 passwords)	☒
• Automatic locking of user accounts after multiple incorrect password entry	☒
• Reasonably secure password reset procedure	☒
Encryption of networks	☒
Locking of data processing systems (e.g. locked cage for servers)	☒
Blocking of external interfaces (e.g. USB)	☒
Program Review and Release Procedures for New Installations	☒
Use of intrusion prevention systems	☒
Use of VPN technology	☒
Use of anti-virus software: Server	☒
Use of anti-virus software: Clients	☒
Use of a software firewall	☒
Use of a hardware firewall	☒
Mobile-Device-Management	☒
Storage of personal data/data carriers in lockable security cabinets or in separately secured rooms	☒
Regulations on home office / teleworking	☒
Other measures: Click here to enter text.	☐

1.3 Access control Intended to prevent unauthorised activities in data processing systems outside of granted authorisations.	**Available**
Use of a role-based authorization concept	☒
Regular reviews of assigned user permissions	☒
Minimal use of administrator accounts	☒
Separation of authorization authorization (organizational) and authorization assignment (technical)	☒
Regulation for restoring data from backups (who, when, at whose request)	☒
Storage of data backups (e.g. tapes, CDs) in the access-protected safe	☐
Restriction of the free and uncontrolled possibility of querying databases	☒
Regular evaluation of logs (log files)	☒
Time limitation of access options	☒
Partial access options to data sets and functions (Read, Write, Execute)	☒
File Access Logging	☐
File deletion logging	☐
File modification logging	☐
Intrusion-Detection (IDS)	☒
• Security Information and Event Management (SIEM) Software	☒
Limited access to log files (log admin only)	☒
Storage of log files on dedicated log file server	☒
Encrypted storage of data	☒
Shredder (Cross-Cut, mindestens Stoves 3, DIN 66399)	☒

Sealed metal containers (so-called data protection bins), disposal by service providers	☒
Data Carrier Disposal - Secure Deletion of Data Carriers (DIN 66399):	☒
Physical destruction (e.g. shredder for particle sizes up to max. 1000 square millimeters)	☒
Demagnetization by thermal destruction (heating of the magnetic disk surface beyond the Curie temperature of the coating used)	☒
Data Destruction Policy	☒
Clean Desk-Policy	☒
Clean Screen Policy	☒
Other measures: Click here to enter text.	☐

1.4 Order control To ensure that data processed on behalf of service providers (subcontractors) is only processed in accordance with the instructions of the client.	**Available**
Drafting of contracts in accordance with legal requirements (Art. 28 GDPR)	☒
Central recording of existing service providers (uniform contract management)	☒
Preliminary checks at the contractor's premises before the start of the contract	☒
Regular inspections at the contractor after the start of the contract (during the duration of the contract)	☒
On-site inspections at the contractor's premises	☒
Review of the data security concept at the contractor	☒
Review of existing IT security certificates of the contractors	☒
Contractor has appointed data protection officer	☒

Issuing instructions to contractors to improve data protection	☒
Other measures: Click here to enter text.	☐

1.5 Separation control Data collected for different purposes must also be processed separately from each other.	**Available**
Separation of customers (multi-client capability of the system used)	☒
Physical data separation (e.g. different systems or data carriers)	☒
Logical data separation (e.g. based on customer or client numbers)	☒
Data backups of client data on separate data carriers (without data from other customers)	☒
Authorization concept that takes into account the separate processing of client data from data of other customers	☒
Separation of development, test and production system	☒
Mapping records to purpose attributes	☒
In the case of pseudonymised data: separation of the mapping file & storage on another system	☒
Other measures: Click here to enter text.	☐

2 Measures to ensure integrity

2.1 Transfer control To ensure the security of data during electronic transmission and data transport and the traceability of the transfer.	**Available**
How is data transferred between the controller and third parties?	

• VPN connection	☒
Email encryption	☒
• SMIME	☒
• OpenPGP	☐
• Sending e-mails with encrypted ZIP files	☒
Data exchange via https connection	☒
- TLS 1.2	☒
Other type of mailing: adHoc module of Move-It	☒
Use of signature procedures	☒
Signature method used: HSM	
Digitally Signing Macros	☒
Documented management of data carriers, inventory control	☒
Encryption of confidential data records	☒
Encryption of mobile data carriers (e.g. laptop hard drives, external hard drives, USB sticks)	☒
Prohibition of carrying bags and other luggage as well as mobile phones into security areas	☒
Regulation on the Making of Records Copies	☒
Backing up disks that need to be transported	☒
Documentation of the bodies to which a transfer is planned and the transmission channels	☒
Direct pick-up, courier service, transport escort	☒
Completeness and correctness check	☒
Other measures: Click here to enter text.	☐

2.2 Input control To ensure that it can be traced whether, who and when personal data has been entered, changed or deleted in data processing systems.	**Available**
Technical logging of data entry, modification and deletion	☒
Manual or automated evaluation of the logs	☒
Differentiated user permissions:	☒
• Individual usernames, not user groups	☒
• Assignment of rights to enter, modify and delete data on the basis of an authorization concept	☒
• Field access to databases	☒
Organizational definition of submission responsibilities	☒
Dedicated log server	☒
Regulation of access authorizations for log servers (LogAdmin)	☒
Regulation on retention periods for auditing/verification purposes	☒
Other measures: Click here to enter text.	☐

3 Measures to ensure availability and resilience

3.1 Availability check Intended to protect data against accidental destruction or loss.	**Available**
Fire alarm systems in server rooms	☒

Smoke detectors in server rooms	☒
Fire doors	☒
Waterless fire suppression systems in server rooms	☒
Water sensors in server rooms	☒
Lightning/surge protection	☒
Air-conditioned server rooms	☒
Server rooms in separate fire compartment	☒
Accommodation of backup systems in separate rooms and in separate fire compartment	☒
Server rooms not under or next to sanitary facilities	☒
Restriction of access to server rooms to necessary personnel	☒
Alarm message in case of unauthorized access to server rooms	☐
Storage of archive storage media under necessary storage conditions (air conditioning, protection requirements, etc.)	☒
CO2 fire extinguisher in the immediate vicinity of the server rooms	☒
UPS system (uninterruptible power supply)	☒
Stromgenerator	☐
Fireproof cabinets	☐
Privacy Vault	☒
Documented data backup and backup concept	☒
Execution of data backups and creation of backups using a central back-up server	☒
Monitoring of the back-up process by helpdesk	☒
Regular data recovery testing	☒
Extensive documentation and plans to restore business operations	☒

Mirroring of the hard disks (e.g. RAID) depending on the protection class	☒
Separate partitions for operating system and data	☒
Average archive (outsourcing of data)	☒
Emergency plan in place (BSI Standard 100-4)	☒
Ensure long-term technical readability of backup storage media	☒
Other measures: Click here to enter text.	☐

3.2 Resilience (resistance and failure control) To enable systems to deal with risk-related changes and to demonstrate tolerance and compensatory capacity for disruptions.	**Available**
Redundant power supply	☐
Uninterruptible power supply to bridge power outages for all central systems	☒
Redundant data connection	☒
Redundant air conditioning in the data center	☒
Alternate data centers available (hot or cold stand-by?): Backup data center available	☒
Other redundant systems/procedures:	☐
Use of a highly available storage area network (SAN) solution	☒
Computer Emergency Response Team (CERT)	☒
Use of load balancing	☒
Delineation of critical components	☒
Conducting penetration tests	☒

System hardening (deactivation of unnecessary components)	☒
Immediate and regular activation of available software and firmware updates	☒
Regular sensitization of employees (at least annually)	☒
Process for immediate reporting of incidents to IT is known to all employees	☒
Taking out cyber insurance	☒
Other measures: Click here to enter text.	☐

4 Measures for periodic review, evaluation and evaluation

4.1 Procedures To ensure the effectiveness of data security measures.	**Available**
Processing records (Art. 30 I and II GDPR) are updated annually	☒
Notification of new/changed data processing procedures to the data protection officer	☒
Notification of new/changed data processing procedures to the IT security officer	☒
Processes for reporting new/changed procedures are documented	☒
Testing of the effectiveness of safety measures taken at least once a year	☒
In the case of negative findings within the framework of the previously gen. the security measures are adapted according to the risk	☒
Process for responding to security breaches (attacks) and system disruptions exists (incident response management)	☒
Documentation of security incidents and documented process for them	☒

4.2 Other Data Protection Management	Available
Using privacy-friendly software settings	☒
Use of data protection management software	☐
Data protection officer appointed	☒
IT security officer appointed	☒
Documented process for dealing with data protection incidents	☒
Clear responsibilities in handling privacy and security incidents	☒
Documented process to ensure the rights of data subjects	☒
Centralised storage of guidelines/procedures accessible to all employees	☒
Periodic checks by the data protection officer	☒
Regular coordination between the Board of Directors and the Data Protection Officer	☒
Regular internal and external audits	☒
Extensive guidelines for employees in the Data Protection Handbook	☒
Annual employee training	☒
Data protection and data security-relevant certifications according to ISO 9001 and ISO 27001 and VDA TISAX	☒
Other measures: Click here to enter text.	☐

SCHEDULE 3 – SUB-PROCESSORS LIST

1. **BMC Software GmbH**

Heriotstrasse 1, 60528 Frankfurt (UE)
Ticketing processing, first-level support

2. **Adobe Systems Software Ireland Ltd.**

4-6 Riverwalk, Citywest Business Campus, Dublin (UE)
Digital signing of documents

3. **Axsos AG**

Konrad-Zuse-Weg 1, 72555 Metzingen (UE)
Service provider platform for e-learning tool