AGREEMENT ON DATA PROCESSING

according to art. 28 GDPR

between

ASC Technologies AG
Seibelstrasse 2-4
63768 Hoesbach
Germany
– hereinafter referred to as ‘Data Processor’ –

and

You as Licensee
– hereinafter referred to as ‘Data Controller’ –

called “Party” individually or “Parties” collectively.

1. Preamble

This Agreement on Data Processing (hereinafter referred to as "Agreement") supplements the underlying main contract and related Service Agreements in terms of data protection law. In terms of its regulatory content and together with its attachments (where applicable), it takes precedence over all other contracts, agreements, and arrangements.

This Agreement governs the implementation of the legal requirements with regard to REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27th April 2016 on the protection of natural persons with regard to the processing of personal data, on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, in short “GDPR”), art. 4 no. 2 and art. 28, of the German Federal Data Protection Act of 30th June 2017 (“BDSG”) and other relevant German legal provisions.

Data processing (“Service”) shall take place exclusively in a member state of the European Union. Any transfer of the service or of part of it to a third country requires the prior consent of the Data Controller and may only take place if the special requirements of art. 44 et seqq. GDPR (e. g. adequacy decision by the commission, standard data protection clauses, BCRs) are fulfilled. If other data processors are supposed to be contracted, these requirements shall apply in addition to the provisions in section 5 of this Agreement.

This Agreement enters into force upon signature of the Data Controller. The Parties agree that once this Agreement between the Parties on the same subject matter enters into force, possibly existing Agreements on data processing will be revoked by mutual agreement and replaced by this new Agreement.

2. Subject of the Agreement

Underlying main contract:	Temporary or permanent assignment of software licenses, service agreement or subscription of an ASC cloud service.
Description of the subject of the contract:	In case of on-premise installations and so-called “Cloud Solutions for Service Providers”: Carrying out installations and support of installations. Verification, modification, expansion, and conversion of hardware and software systems. Fulfilment of service agreements across several organizational levels (“1st – 2nd – 3rd level”) for fault identification and troubleshooting. Software maintenance by means of updates and upgrades. Management of inventory data and databases on instruction of the Data Controller. In case of ASC cloud services: Provision, operation, and maintenance of such service within the scope of the selected subscription and within the Microsoft Azure Cloud.
Begin and duration of the contract:	Generally: In accordance with the main contract, service agreements, and terms of use and license. In case of ASC cloud services: During the term of subscription.
Scope, type and purpose of the intended processing of data:	Collection, transmission, and evaluation of log files within the scope of system interventions of the Data Controller or its customers are carried out by means of on-site intervention or by means of access via remote data transmission ("Remote Service”). These log files and additional system information are required to fulfill the subject of the contract. They may contain personal communication data, log data as well as access and authorization information. The personal telecommunication contents and other inventory data which have been recorded and evaluated on the systems of the Data Controller or its customers with the products of the Data Processor installed there, are processed only on the express instruction on behalf of the Data Controller.
Data categories:	Log files, system/access/authorization information, communication content. Company and contact data.
Categories of data subjects:	Employees, customers, prospects, business partners, suppliers, public institutions/authorities.

2.1 The Data Controller is the data owner according to art. 4 no. 7 GDPR and art. 24 GDPR. The Data Controller is responsible for compliance with the applicable provisions, particularly for the legality of data processing, the legality of data transfer to the Data Processor, the information duties, the provision of information, and the fulfilment of requests for erasure.

2.2 The Data Processor commits itself to comply with the legal provisions and to support the Data Controller with the above-mentioned requirements upon request.

2.3 The Data Controller may terminate this Agreement at any time and without notice if the Data Processor severely breaches the provisions of the underlying main contract or of this Agreement, if the Data Processor is unable or unwilling to comply with the instructions given by the Data Controller, if the Data Processor violates the GDPR or other data protection regulations, or if the Data Processor breaches this Agreement by refusing the Data Controller its rights to data control.

3. Rights and Obligations of the Data Controller

3.1 The Data Controller places all orders or partial orders in writing or in a documented electronic format. Changes to the subject of processing and changes to procedures shall be agreed jointly and defined accordingly in writing or in a documented electronic format. The Data Controller shall ensure that all orders and partial orders – insofar as they do not comply with the table in section 2 of this Agreement – contain information about the following points:

a) Subject and purpose of processing

b) Type and purpose of the intended processing of data

c) Type of the personal data

d) Categories of data subjects

3.2 The Data Controller has the right to issue instructions to the Data Processor at any time. Instructions must be given in writing or by e-mail; oral instructions shall be confirmed immediately in writing or in a documented electronic format. In case the Data Controller is a Data Processor to a Controller higher in the process chain, he must, upon request of the Data Processor, submit a confirmation of this superior Controller for critical instructions such as the erasure of data or prove its existence in a justiciable manner and with discharging effect for the Data Processor.

3.3 If the Data Controller's instructions are not covered by the contractually agreed scope of services, they shall be treated as a request to change the scope of services. In the event of suggestions for change, the Data Processor shall inform the Data Controller of the effects on the agreed services, particularly the possibility of service provision, deadlines, and remuneration. If the Data Processor cannot reasonably be expected to comply with the instructions, the Data Processor is entitled to terminate the processing. In all other respects, the service descriptions and the respective contractual agreements shall apply.

3.4 The Data Controller’s authorized persons to issue instructions and the recipients of instructions at the Data Processor’s place (“Contact persons”) are listed in Attachment 1. If the contact person of one Party changes or is unavailable for a longer period of time, the other Party must be informed about the successor or representative in writing or electronically. If instructions change, revoke, or amend the previous contractual provisions, they are only permissible if a corresponding new provision is made. Instructions must be stored for their period of validity and subsequently for another three (3) calendar years.

3.5 The Data Controller is responsible for ensuring that the technical and organizational measures at the Data Processor’s place (see also section 6) for the risks of the data to be processed offer an appropriate level of protection. Before the start of the data processing and thereafter in regular appropriate intervals, the Data Controller is therefore entitled to inspect the compliance with the measures taken by the Data Processor as well as with the obligations laid down in this Agreement (art. 32 par. 1 lit. d GDPR). The result of the inspections must be communicated to the Data Processor in writing.

3.6 The Data Controller shall immediately inform the Data Processor upon detecting errors or irregularities in the examination of the processing results.

3.7 The Data Controller is bound to treat all knowledge of trade secrets and data security measures of the Data Processor acquired within the scope of this Agreement confidentially. This obligation shall continue to apply even after termination of this Agreement.

4. Rights and Obligations of the Data Processor

4.1 The Data Processor shall process personal data only within the framework of the concluded agreements and according to the instructions of the Data Controller unless obliged to do so by the law of the European Union or the Member States to which the Data Processor is subject (e. g. investigations by law enforcement or state protection authorities); in such a case, the Data Processor informs the Data Controller of these legal requirements prior to data processing unless the law in question prohibits such notification on the grounds of an important public interest (art. 28 par. 3 lit. a GDPR). The Data Processor has to correct, delete, and block personal data if the Data Controller requests this in the concluded Agreement or in an instruction. The Data Processor does not use the data provided for data processing for any other purposes than the agreed ones, especially not for own purposes. No copies or duplicates are made without the knowledge of the Data Controller.

4.2 If data carriers are used which come from the Data Controller or are used for the Data Controller, they will be marked separately. Receipt and delivery as well as the current use are documented.

4.3 In the area of the contractual processing of personal data, the Data Processor guarantees that all agreed measures will be carried out according to the Agreement. He assures that the processed data will be strictly separated from other data.

4.4 The Data Processor shall cooperate to the necessary extent with the Data Controller in complying with the rights of the data subjects according to art. 12 to 22 GDPR, in creating a list of processing activities according to art. 30 sec. 1 GDPR as well as in the required assessing of the data protection impact by the Data Controller according to art. 35 GDPR and provide the Data Controller with appropriate support wherever possible (art. 28 par. 3 lit. e and f GDPR). Upon request by the Data Controller, the Data Processor shall forward the required information without delay to the persons responsible at the Data Controller’s place named in Attachment 1, particularly also to the Data Protection Officer (DPO) there. The Data Processor is entitled to demand an appropriate remuneration from the Data Controller for these cooperation and support services.

4.5 The Data Processor shall immediately notify the Data Controller when suspecting that an instruction given by the Data Controller infringes legal regulations (art. 28 par. 3 GDPR). The Data Processor is entitled to suspend the execution of the respective instruction until it is confirmed or changed by the person responsible at the Data Controller’s place.

4.6 Information about personal data from the contractual relationship to third parties or the parties concerned may only be provided by the Data Processor after prior instruction or approval by the Data Controller. In the absence of the Data Controller's approval, the Data Processor shall immediately refer persons entitled to information and those affected to the Data Controller as the one responsible for providing information. The Data Processor may only provide employees of the Data Controller with information if they are the respectively authorized persons (see Attachment 1).

4.7 The Data Processor shall immediately inform the Data Controller about any disturbances and violations by the Data Processor or its employees of data protection regulations or the specifications stipulated in the order as well as about suspected data protection violations or irregularities in the processing of personal data.

4.8 This applies above all to any reporting and notification obligations of the Data Controller according to art. 33 and art. 34 GDPR. The Data Processor assures to adequately support the Data Controller in its obligations according to art. 33 and art. 34, if required (art. 28 par. 3 lit. f GDPR). Notifications according to art. 33 or art. 34 GDPR for the Data Controller may only be made by the Data Processor after prior instruction according to clause 3 of this Agreement.

4.9 The Data Processor immediately informs the Data Controller about control actions, examinations, and measures of the supervisory authority according to art. 58 GDPR. This also applies if a responsible authority conducts investigations at the Data Processor’s place.

4.10 If there are changes in operating procedures, e. g. during the exchange of hardware and software, the Data Processor shall ensure that no data of the Data Controller is passed on to third parties or that it has been deleted in accordance with data protection regulations before transfer.

4.11 The Data Processor agrees that the Data Controller is entitled - exclusively by appointment - to check compliance with the provisions on data protection and data security as well as with the contractual agreements to the necessary and appropriate extent personally or to commission third parties to do so, particularly by obtaining information and by carrying out inspections on site (art. 28 par. 3 lit. h GDPR). The Data Processor guarantees assistance in these inspections, where required. The Data Processor is entitled to demand an appropriate remuneration from the Data Controller for providing information and tolerating or supporting these inspections.

4.12 Safety-relevant decisions regarding the organization of data processing and the deployed procedures shall be agreed upon with the Data Controller in advance.

4.13 The name of the DPO of the Data Processor is included in Attachment 1; the Data Controller must be informed immediately about any changes.

4.14 The Data Processor undertakes to maintain confidentiality when processing the Data Controller's personal data according to the contract. Confidentiality shall continue to apply even after termination of the Agreement. The Data Processor confirms that it is aware of the relevant legal regulations, particularly of telecommunications secrecy according to § 3 TTDSG.

4.15 The Data Processor warrants that it will (i) familiarize the employees involved in carrying out the tasks before they start working with the data protection provisions applicable for them by means of trainings according to art. 39 par. 1 lit. b GDPR; (ii) obligate them to confidentiality in an appropriate way for the duration of their task as well as after the termination of their employment (art. 28 par. 3 lit. b and art. 29 GDPR); and (iii) monitor the compliance with the confidentiality provisions appropriately.

4.16 Thirty (30) days after the completion of the commissioned data processing, the Data Processor shall completely and irrevocably delete all personal data provided to it under this Agreement in all its systems (including all copies, also in archiving and backup files) (art. 28 par. 3 lit. g GDPR). For a fee, the Data Processor shall make all data processed on behalf available to the Data Controller for secure downloading between the completion of data processing and final deletion. The Data Controller shall receive a written or electronically documented confirmation of the data’s deletion in compliance with data protection law.

5. Sub-Processors (art. 28 par. 3 lit. d GDPR)

5.1 Latest when this Agreement enters into force, the Data Processor will contract the sub-processors listed in Attachment 1.

5.2 The Data Controller grants the Data Processor the general authorization to commission other sub-processors. The Data Processor shall inform the Data Controller in advance about any intended change in relation to involving other sub-processors for the first time or to the replacement of existing other data processors. The Data Controller may object to such an intended change in writing or in a documented electronic format within four (4) weeks of receipt of the notification and is granted a special right of termination due to this fact.

5.3 Sub-processors in third countries may only be commissioned with data processing if the special requirements of art. 44 et seqq. GDPR (e. g. adequacy decision by the commission, standard data protection clauses, BCRs) are fulfilled.

5.4 The Data Processor guarantees that sub-processors have been selected carefully with special regard to their suitability in terms of the technical and organizational measures taken within the meaning of art. 32 of GDPR.

5.5 Any agreement with sub-processors shall be in writing which may also be in an electronic format (art 28 par. 4 and par. 9 GDPR).

5.6 The Data Processor shall contractually ensure that the agreed regulations between the Data Controller and the Data Processor also apply mutatis mutandis to sub-processors and shall be liable to the Data Controller for compliance therewith.

5.7 The transmission of data is only permitted if a sub-processor has fulfilled the obligation according to art. 29 and art. 32 par. 4 GDPR with regard to its employees. The details especially of the scope, type, and purpose of data processing as well as regarding sections 4.7 and 5.2 shall be specified in the agreement with the sub-processor in such precision that the responsibilities of the Data Processor and of the sub-processor are clearly distinguished. If several sub-processors are commissioned, this shall also apply to the responsibilities between these sub-processors.

6. Technical and Organizational Measures (art. 32 GDPR in conjunction with art. 28 par. 3 lit. c GDPR)

6.1 A level of protection appropriate to the risk for the rights and freedoms of the natural persons affected by the processing is guaranteed for the specific data processing. To this end, the protection objectives of art. 32 (1) GDPR such as confidentiality, integrity, and availability of systems and services as well as their resilience with regard to the type, scope, circumstances, and purpose of processing, are taken into account in such a way that the risk is permanently contained by appropriate technical and organizational measures.

6.2 The technical and organizational measures of the Data Processor described in Attachment 1 shall be deemed sufficiently approved by the Data Controller. They may be reasonably developed further and modified by the Data Processor over time but must not fall below the agreed standards. The Data Processor shall coordinate essential changes with the Data Controller in documented form.

6.3 If the technical and organizational measures taken by the Data Processor do not meet the Data Controller's requirements, the Data Controller shall inform the Data Processor without delay. The Data Processor may charge the Data Controller for the cost of any subsequent improvements that exceed a reasonable extent.

6.4 All agreements on technical and organizational measures as well as control and audit documents (also on other data processors) shall be kept for the period of validity of this Agreement and subsequently for another three (3) full calendar years unless legal requirement stipulate a longer retention period.

7. Miscellaneous

7.1 This Agreement – together with the applicable Attachments – constitutes the entire agreement between the Parties in this respect; no oral collateral agreements have been made.

7.2 All amendments and supplements to this Agreement must be made in writing; this shall also apply to the amendment of the written form requirement.

7.3 Should one of the provisions of this Agreement be or become invalid, this shall not affect the validity of the remaining provisions. In such a case, the Parties shall be obliged to cooperate in the creation of conditions that achieve a legally valid result that comes as close as possible to that of the invalid provision. The foregoing shall apply mutatis mutandis to the closing of any loopholes in the Agreement.

7.4 This Agreement shall be governed by the laws and jurisdiction of the Federal Republic of Germany.

<u>The following attachments become an integral part of this Agreement:</u>

Attachment 1: Technical and organizational measures according to art. 32 GDPR, authorized individuals and sub-processors

1. Description of Technical and Organizational Measures taken by the Data Processor in accordance with art. 32 GDPR

1.1 Confidentiality (art. 32 par. 1 lit. b GDPR)

a) Admittance Control

No unauthorized admittance to data processing systems, e. g. by means of magnetic or chip cards, keys, electric strikes, plant security or gatekeepers, alarm systems, video systems.

<u>The Data Processor has implemented the following technical and organizational measures:</u>

- Automatic admittance control system with logging.
- Primary chip cards/transponder lock systems with electric motorized locks.
- Additional manual lock system with security locks as well as regulation on handing out/returning keys.

Admittance of external persons is regulated:

- You are only admitted to the office building upon calling at the reception where you will be picked up by an employee and accompanied at all times. Admittance to security-critical areas is not granted and, if objectively necessary, will only take place in company and under the constant supervision of authorized persons.
- Structural measures ensure a separation between public and employee traffic. Areas reserved exclusively for employees can only be accessed via an admittance control system which logs the accesses.
- Cleaning staff works during office hours only and thus under supervision.

Security-critical areas (e. g. server rooms, UPS location) have been structurally secured; only a strictly limited group of people is admitted.

An alarm system/burglar alarm system monitors security-relevant areas upon activation (automatically Mon-Fri from 22:00 - 06:00 o'clock and on weekends) via infrared motion detectors and video cameras. The alarm system is connected to a security service 24/7; in the event of an alarm, it is connected via cameras and an intercom system. In the event of insufficient identification, an alarm is sent to the police and a contact person of ASC.

b) Admission Control

No unauthorized usage of the system, e. g. by means of secure passwords, automatic locking mechanisms, two-factor authentication, encryption of data carriers.

<u>The Data Processor has implemented the following technical and organizational measures:</u>

- Personal authorizations, limited to the extent necessary to fulfill the task ("need-to-know" principle).
- Usage of individual-related usernames in Microsoft Azure Active Directory hosted user accounts.
- Authentication by means of username/password. Single sign-on to workstations and servers not possible.
- User- and system-dependent two-factor authentication is enforced via dedicated smartphone.
- Password guideline according to BSI guideline (length, complexity, frequency of changes, history).
- Assignment of user profiles to IT systems (separation of roles).
- Usage of a hardware firewall, additional software firewall on all workstations and servers.
- Usage of VPN technology (AES-256-CBC, 2048 bit).
- Usage of active intrusion prevention systems (firewall).
- Encryption of mobile data carriers on demand (minimum is AES-256 hardware encryption or Bitlocker-to-go).
- Encryption of data carriers in laptops (Full-disk encryption by means of SSD firmware or Microsoft Windows Bitlocker).
- Usage of a central smartphone administration software (e. g. remote erasure).
- Screen lock, manual or enforced (default ten minutes).
- Organization instruction for the secure storage of documents and mobile data carriers.

c) Access Control

No unauthorized reading, copying, modification or removal in the system, e. g. by means of authorization concepts and access rights according to requirements, logging of accesses.

<u>The Data Processor has implemented the following technical and organizational measures:</u>

- Personal authorizations, limited to the extent necessary to fulfill the task ("need-to-know" principle).
- Administration of rights by particularly obliged system administrators based on dual control.
- Number of administrators is limited to a minimum.
- Password guideline according to BSI guideline (length, complexity, frequency of changes, history).
- Logging of access to applications, especially when entering, changing, and deleting data.
- Secure storage of data carriers.
- Encryption of data carriers on demand.
- Proper destruction of data carriers (DIN 66399), logging.
- Proper destruction of paper (using shredders or employing service providers), logging.
- Usage of anti-virus software.
- Implementation of "clean-desk policy".

d) Separation Control/Usage Control

Separate processing of data which has been collected for different purposes, e. g. by means of multi-tenant capability, sandboxing.

<u>The Data Processor has implemented the following technical and organizational measures:</u>

- Logically separated storage on the same systems/Separation of tenants.
- If required, separate storage on separate data carriers.
- Separation of productive systems and test systems.
- Separation of productive and test system networks.

e) Pseudonymization and Encryption (art. 32 par. 1 lit. a GDPR; art. 25 par. 1 GDPR).

Processing of personal data in such a way that the data can no longer be associated with a specific data subject without using additional information, provided that this additional information is kept separately and subject to appropriate technical and organizational measures.

<u>The Data Processor has implemented the following technical and organizational measures:</u>

- Possibility of processing data in pseudonymized/anonymized form.
- Separation of the file used for data association as well as storage on a separate, secured system/data carrier.
- Previous approval in case of re-association of pseudonyms on basis of separate access authorizations.
- Appropriate controls to verify efficiency.
- For further information about encryption for (electronic) transport see Transfer control (see 1.1. d).
- Encryption measures for storage in a database container.
- Encryption on basis of relevant standards (e. g. RSA, AES-256 Bit).
- Recording data in ASC Recording Insights can alternatively be encrypted using a customer's own Azure key (BYOK).

1.2 Integrity (art. 32 par. 1 lit. b GDPR)

a) Transfer Control

No unauthorized reading, copying, modification or removal during electronic transmission or transport, e. g. by means of encryption, Virtual Private Networks (VPN), electronic signature.

<u>The Data Processor has implemented the following technical and organizational measures:</u>

- Installation of fixed site-to-site VPNs.
- Encrypted data transmission (e. g. via https:// or SFTP).
- E-mail encryption according to the latest TLS standard as far as technically possible on the opposite site Inboxes hosted in Microsoft Office 365 Tenant.
- Encryption of external data carriers such as hard disks, CDs, USB sticks (minimum is AES-256 hardware encryption or Bitlocker-to-go).
- Logging of connection data upon data transmission.
- Definition of authorized groups of people for different topics and situations (separation of roles).
- During physical transport: Secure transport containers and packaging as well as careful selection of transport companies and transport personnel

b) Entry Control

Determining whether and by whom personal data has been entered, modified, or removed in data processing systems, e. g. by means of logging, document management.

<u>The Data Processor has implemented the following technical and organizational measures:</u>

- Intrasystem logging of the entry, modification, and deletion of data (Omnitracker).
- Defined responsibilities in an authorization concept, including process documentation within the framework of the ASC multi-management system for assigning rights as well as entering, changing, and deleting data.
- Traceability by means of individual-related usernames/passwords.

1.3 Availability and Resilience (art. 32 par. 1 lit. b GDPR)

a) Availability Control

Protection against unintentional or intentional destruction or loss, e. g. by means of a backup strategy (online/offline; on-site/off-site) uninterrupted power supply (UPS), virus protection, firewall, reporting channels, emergency plans.

<u>The Data Processor has implemented the following technical and organizational measures:</u>

- Creating of a backup and recovery concept.
- Regular backup of system states.
- Regular backup of data pools.
- Regular backup of databases.
- Storage of data backups in a secure, outsourced location, in fire- and water-proof safety cabinets; vaults for the storage of data backups are protection class S 60 DIS.
- Storage of data backups in a different fire compartment.
- Creating of an emergency plan/concept.

- Regular update of software inventory.
- Uninterruptable power supply (UPS) and overvoltage protection.
- Air conditioning in server rooms.
- Devices to monitor temperature, humidity as well as CO/CO_2 in server rooms.
- Protected socket strips in server rooms.
- Fire- and smoke-detection systems.
- Fire-extinguishing equipment in server rooms.
- Alarm messages in case of unauthorized access or access attempts to server rooms, see also 1.1 a)
- No server rooms under sanitary facilities or under water or drainpipes.

b) Resilience of Systems

The risk of destruction, loss, modification, unauthorized disclosure or unauthorized admission due to system overloads or crashes shall be reduced.

The Data Processor has implemented the following technical and organizational measures:

- Monitoring of operation parameters, usage of service, and system utilization.
- Emergency concept.
- Usage of redundant systems/components (hardware).
- Manufacturer diversification for protection components (hardware and software).
- Measures to fend off attacks (e. g. virus scanner, firewall).
- Regular prognosis of future usage and timely adjustment of the systems’ capacities.
- Dimensioning of the storage, access, and performance capacities of the systems and services during times of scheduled or predicted peak load.
- Usage of error-tolerant systems.

c) Quick Restoration of Availability and Access (art. 32 par. 1 lit. c GDPR)

The Data Processor has implemented the following technical and organizational measures:

- Restoration according to backup and recovery concept.
- Testing reconstruction of data.

1.4 Process for regularly Testing, Assessing, and Evaluating Effectiveness (art. 32 par. 1 lit. d GDPR; art. 25 par. 1 GDPR)

a) Data Protection Management

The Data Processor has implemented the following technical and organizational measures:

- Binding company-wide data protection guideline.
- Procedure instruction on data protection within the ASC multi-management system.
- Regular internal data protection audits.
- Control system which blocks unauthorized access or access attempts.
- Directory of processing activities exists and is up to date.
- Appointment of a Data Protection Officer (TÜV-certified).
- Appointment of an Information Security Officer (TÜV-certified).
- Involvement of Data Protection Officer and Information Security Officer in data protection impact assessment and Compliance Committee.
- Regular employee trainings on data protection laws.
- Obligation of employees to confidentiality when handling personal data.
- Obligation of employees to telecommunications secrecy.

b) Incident Response Management

Process of how to react to detected or suspected security incidents or disorders in IT areas as well as preventive measures and processes.

The Data Processor has implemented the following technical and organizational measures:

- Process of how to deal with incidents and to meet reporting deadlines towards data subjects and regulating authorities.

c) Data Protection by Design and by Default (art. 25 par. 2 GDPR)

The Data Processor has implemented the following technical and organizational measures:

- Observation of the principle of data protection by design (“privacy by design”)
- Observation of the principle of data protection by default (“privacy by default”)

d) Order Control/Involvement of Sub-Processors

No data processing in terms of art. 28 GDPR without the authorization of the Data Controller, e. g. unambiguous contract design, formalized order management, strict selection criteria for service providers, obligation to obtain prior permission, subsequent checks.

The Data Processor has implemented the following technical and organizational measures:

- Careful selection of other data processors with regard to implemented technical and organizational measures (TOMs) and providing sufficient guarantees.
- Previous and regular - at least on a sample basis - check of the Data Processor and its activities with regard to the implemented TOMs and the contractually agreed purpose of processing.
- Formal order incl. contractual agreement on data processing.
- Documentation of the services and obligations of the Data Processor and the Data Controller.
- Efficient control rights have been stipulated.
- All instructions have been documented in writing.
- Data Processor has appointed Data Protection Officer.
- Obligation of the employees of the Data Processor to confidentiality or data secrecy and telecommunications secrecy.
- Guarantee to return and/or destroy the data upon the completion of the order.

1.5 Documentation (art. 32 par. 1 GDPR; art. 25 par. 1 GDPR)

- Guideline on Information Security and Data Protection (MMGL-4600).
- Code of Conduct and declarations of commitment.
- Other manuals, guidelines/rules of conduct, procedural and work instructions, process documentation, functional descriptions, risk analyses and assessments and other relevant control and verification documents as part of the TÜV-certified multi-management system.

1.6 Certifications / Attestations

- DIN EN ISO 9001:2015
- DIN EN ISO 14001:2015
- DIN EN ISO/IEC 27001:2017
- ISAE-3402 / SOC-2

2. Data Protection Officers

2.1 Data Processor

Name, First name.	**Haßkerl, Kilian**
Phone	+49 6021 5001-316
E-mail	data.protection@asc.de

2.2 Data Controller

THE DATA CONTROLLER IS OBLIGATED TO PROVIDE ASC WITH THE CONTACT DATA OF ITS DATA PROTECTION OFFICER (IF APPOINTED) IN WRITING AND UNSOLICITED WHEN THIS AGREEMENT COMES INTO FORCE, AND TO UPDATE SUCH INFORMATION IN THE EVENT OF LATER CHANGES. WITHOUT SUCH INFORMATION ON HAND, ASC **MAY** REFUSE TO CARRY OUT DATA PROTECTION INSTRUCTIONS FOR SECURITY REASONS.

2.3 Responsible Regulatory Authority

Name	**Bavarian Authority for Data Protection Supervision**
Home address	Promenade 18, DE 91522 Ansbach
Postal address	P.O. Box 1349, DE 91504 Ansbach
Country	Germany
Phone / Fax	+49 981 180093-0 / +49 981 180093-800
E-mail	poststelle@lda.bayern.de

3. Recipients of Instructions and Persons authorized to issue Instructions

3.1 Data Processor

Name, First name.	**Fengler, Tobias**
Function	Chief Engineering Officer
Phone	+49 6021 5001-355
E-mail	t.fengler@asc.de
Area of authority	Engineering / Service
Name, First name.	**Bieder, Katja**
Function	Head of Service Administration
Phone	+49 6021 5001-246
E-mail	k.bieder@asc.de
Area of authority	Engineering / Service

3.2 Data Controller

THE DATA CONTROLLER IS OBLIGATED TO PROVIDE ASC WITH THE CONTACT DATA OF ITS PERSONS AUTHORIZED TO ISSUE INSTRUCTIONS IN WRITING AND UNSOLICITED WHEN THIS AGREEMENT COMES INTO FORCE, AND TO UPDATE SUCH INFORMATION IN THE EVENT OF LATER CHANGES. WITHOUT SUCH INFORMATION ON HAND, ASC **WILL** REFUSE TO CARRY OUT DATA PROTECTION INSTRUCTIONS FOR SECURITY REASONS.

4. Sub-Processors

4.1 External

Company name	**EUROKEY Software GmbH**
Street	Fischbachstraße 86
ZIP code Place	DE 66125 Saarbrücken
Country	Germany
Phone	+49 6897 79089-0
E-mail	info@eurokey.de
Scope of order	Development services and technical support (3rd level support) for player components
Company name	**EML European Media Laboratory GmbH**
Street	Berliner Straße 45 (Mathematikon)
ZIP code Place	DE 69120 Heidelberg
Country	Germany
Phone	+49 6221 533 323
E-mail	anja.varga@eml.com
Scope of order	Development services and technical support (3rd level support) for keyword spotting / transcription

Company name	**1&1 Internet SE**
Street	Elgendorfer Straße 57
ZIP code Place	DE 56410 Montabaur
Country	Germany
Phone	+ 49 2602 96008162-0
E-mail	info@1und1.de
Scope of order	Website hosting (https://www.asc.de), form data is sent by e-mail
Company name	**Microsoft Deutschland GmbH**, Walter-Gropius-Strasse 5, 80807 München, Germany
Scope of order	▪ Microsoft Office 365: Office applications (e-mail, calendar, contacts, word processing, spreadsheets, OneDrive, SharePoint, Teams, etc.). ▪ Microsoft Dynamics 365: Customer Relationship Management. ▪ Microsoft Azure: Azure Active Directory & Azure Domain Managed Services, different virtual servers (IAAS, Azure Web Application Proxy). Microsoft operates the above-mentioned services from the cloud, hosts the respective data, and gives comprehensive security guarantees that ASC can only pass on: ▪ https://privacy.microsoft.com/en-us/privacystatement/ ▪ https://servicetrust.microsoft.com/ ▪ https://azure.microsoft.com/en-us/support/legal/ ▪ https://www.microsoft.com/en-us/trust-center/product-overview/

4.2 Internal (majority-owned Affiliates under full operational control of the Data Processor)

Company name	**ASC Technologies GmbH**
Street	Nell-Breuning-Allee 6
ZIP code Place	DE 66115 Saarbrücken
Country	Germany
Phone	+49 681 844968-0
E-mail	saarbruecken@asctechnologies.com
Scope of order	Software development and technical support (2nd / 3rd level support)
Company name	**ASC Cloud Solutions SRL**
Street	Bulevardul MUNCII Nr. 22 A birou 2.1; Etaj 2
ZIP code Place	RO 500281 Brasov
Country	Rumania
Phone	+40 751 299797
E-mail	brasov@asctechnologies.com
Scope of order	Software development and technical support (2nd / 3rd level support)
Company name	**ASC Technologies S.R.L.**
Street	Via Privata Santi Nabore e Felice 7
ZIP code Place	MI 20147 Milano
Country	Italy
Phone	+39 02 4802 7177
E-mail	italy@asctechnologies.com
Scope of order	Software development and technical support (2nd / 3rd level support)