Data Processing Agreement

between

Controller

adress

– hereinafter referred to as "Controller"

and

adventics GmbH

Münchener Str. 23a

85540 Haar bei München

– hereinafter referred to as the "Processor"

and collectively referred to as "the Parties" –

is hereby agreed as follows:

1. Subject matter and Term

The Processor shall carry out the data processing listed in Annex 1. It shall describe the subject matter, nature, purpose and duration of the processing as well as the categories of data processed and data subjects.

2. Instructions by the Controller

(1) The Processor shall process personal data only for the purposes listed in Annex 1 or on documented instructions from the Controller, unless the Processor is required to process certain personal data by law of the Union or a Member State to which the Processor is subject. In such a case, the Processor shall notify the Controller of those legal requirements prior to the processing, unless the law in question prohibits such notification on grounds of substantial public interest.

(2) The Processor shall immediately inform the Controller if, in its opinion, an instruction of the Controller infringes the Union or a Member State data protection law.

(3) Processing of the personal data provided by the Controller for other purposes than listed in Annex 1, in particular for its own purpose, is not permitted.

3. persons authorized to issue instructions to the customer, instructions to the contractor

(1) Persons authorized to issue instructions to the Customer are:

- _____

(2) Persons authorized to issue instructions to the Contractor are:

- Bernhard Gamper, Managing Director, Tel. +49 (89) 4444 33 130, bernhard.gamper@adventics.de

- Gunnar Heinrich, Managing Director, Tel. + 49 (89) 4444 33 140, gunnar.heinrich@adventics.de

(3) Communication channels to be used for instructions:

- Preferably e-mail

(4) In the event of a change or long-term prevention of the contact persons, the Contractual Partner shall be informed immediately and in principle in writing or electronically of the successors or the representatives.

4. Technical and organisational measures

(1) The Processor shall undertake to implement the technical and organisational measures specified in Annex 3 to ensure the security of personal data. The measures shall ensure a level of protection appropriate to the risk involved in processing the data in scope of this Agreement. In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context, purposes of the processing and categories of data (in particular pursuant to Article 9(1) or Article 10 of the GDPR), as well as the different probabilities of occurrence and the severity of the risk for the data subjects.

(2) The technical and organisational measures listed in Annex 3 are subject to technical progress and further development. They shall be adapted by the processor if the agreed level of security can no longer be guaranteed. The adaptation may only be carried out if they at least provide the same level of protection achieved when previous measures were in force. Unless otherwise stipulated, the Processor shall notify the Controller of the adjustments made willingly and without undue delay.

5. Obligations of the processor

(1) The Processor confirms that it is aware of the relevant data protection regulations. The Processor shall organise the internal operating procedures within its area of responsibility in such a way that it meets the special requirements of an effective data protection management program.

(2) The Processor shall grant access to the personal data undergoing processing to only to those employees familiar with the Data Protection Law in force and to the extent strictly necessary for implementing, managing and monitoring of the Agreement. The Processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(3) To the extent required by law, the Processor shall appoint a data protection officer and provide his/her contact details in Annex 1. The Processor shall inform without delay and unrequested about any change of the Data Protection Officer.

(4) The Processor shall carry out the processing in the territory of the Federal Republic of Germany, in a Member State of the European Union or within the European Economic Area. Any transfer of data to a third country by the Processor shall be

done only on the basis of documented instructions from the Controller and shall take place if the specific legal requirements of the GDPR are met.

6. Assistance to the Controller

(1) The processor shall promptly notify the controller of any request it has received from the data subject. The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing.

(2) In addition to the processor's obligation to assist the controller pursuant to Clause 5(1), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

a. the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment');

b. the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

(3) The Processor shall provide assistance in reviewing data breaches and implementing any notification obligations, as well as in complying with the obligation to ensure that personal data is accurate and up to date.

(4) Furthermore, the Processor shall assist with appropriate technical and organisational measures to enable the Controller to fulfil its existing obligations towards the data subject.

7. Use of sub-processors

(1) The Processor has the Controller's general authorisation for the engagement of sub-processors. The Processor shall specifically inform the Controller in writing, of any intended sub-processing or change in sub-processors at least three weeks prior, thereby giving the Controller sufficient time to be able to object to such changes. The Processor shall provide the Controller with the information necessary to enable the Controller to exercise the right to object. The use of the sub-processors listed in Annex 2 shall be deemed to be approved, provided that the prerequisites set out in Section 7(2) of this Agreement are implemented.

(2) Where the Processor engages a sub-processor for carrying out specific processing activities (on behalf of the Controller), it shall do so by way of a written contract, which may also be concluded in an electronic format, which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with the clauses in this Agreement. At the Controller's request, the Processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the Controller. The Processor shall remain fully responsible to the Controller for the performance of the sub-processor's obligations in accordance with its contract with the Processor. The Processor shall notify the Controller of any failure by the sub-processor to fulfil its contractual obligations without undue delay.

(3) The Processor shall ensure compliance with the provisions of Articles 44 to 50 of the GDPR in the event of a subcontracting involving a transfer of personal data within the meaning of Chapter V of the GDPR by providing, where necessary, appropriate safeguards in accordance with Article 46 of the GDPR.

(4) Where the Processor engages a sub-processor in processing activities which involves a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the Processor and the sub-processor shall ensure compliance with Chapter V of GDPR by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) GDPR, provided the conditions for the use of those standard contractual clauses are met.

(5) In the case of Section 7(4), the Processor shall carry out the assessment in accordance with Articles 14 and 15 of the Standard Contractual Clauses and make it available to the Controller upon request. If the Processor or the Controller come to the conclusion that further measures need to implemented to ensure an adequate level of protection, these measures shall be implemented by the Processor or the sub-processor respectively. The sub-processor may only be involved in the data processing once an adequate level of protection has been ensured.

8. Documentation and compliance

(1) The Processor shall provide the Controller with all information necessary to demonstrate compliance with the obligations set out in this Agreement and adapted directly from the GDPR. At the Controller's request, the Processor shall also allow and contribute to audits of the processing activities covered by this Agreement, at reasonable intervals or if there are indications of non-compliance of any required regulations. In deciding on a review or an audit, the Controller may take into account relevant certifications within the meaning of Article 28(5) GDPR held by the Processor.

(2) The Controller may choose to conduct the audit by itself or mandate an independent auditor. The costs for this are covered by the Controller. Audits may also include inspections at the premises or physical facilities of the Processor and shall, where appropriate, be carried out with reasonable notice and in a manner that complies with the Processor's business and confidentiality obligations and, where possible, without disrupting operations.

(3) The Processor warrants that it will assist in these audits to an appropriate extent, if necessary. Expenses incurred for up to 4 hours shall be covered by the Processor. All expenses incurred in excess of this shall be covered by the Controller.

(4) The Parties shall make the information referred to in this Agreement, including the results of any audits, available to the competent supervisory authority/ies on request.

9. Infringements to be notified

(1) The Processor shall inform the Controller without undue delay of any disruptions to operations that entail risks for the Controller's data, as well as when data protection breaches in connection with the Controller's data become known. The

same shall apply if the Processor establishes that the security measures taken by the Processor do not meet the legal requirements.

(2) The Processor is aware that the Controller is under an obligation to comprehensively document all breaches of personal data protection and, if necessary, to report them to the supervisory authority/ies or the data subject. The Processor shall notify the Controller without undue delay after the Processor having become aware of the breach. Such notification shall contain, at least:

- Description of the nature of the breach, including, where possible, the categories and approximate number of individuals and data sets affected,
- Name and contact details of contact persons for further information,
- a description of the likely consequences of the injury, and
- a description of the measures taken or proposed to correct the breach or mitigate the resulting adverse effects.

10. Termination

(1) Following termination of the Agreement, the Processor shall delete or return all personal data processed on the behalf of the Controller unless the Union or a Member State law requires storage of the personal data. This shall also apply to any existing copies in accordance with the technical and organizational measures taken. The Processor shall notify the Controller of the deletion and return of the data in writing.

(2) the Controller may terminate the contractual relationship without notice if the Processor commits a serious breach of the provisions of this Agreement or of data protection regulations and the Controller cannot reasonably be expected to continue the contractual relationship until the conclusion of the notice period or until the agreed termination of the Agreement.

(3) The Processor may terminate the contractual relationship without notice if the Controller insists on the fulfilment of its instructions even though such instructions violate applicable legal requirements or this Agreement and the Processor has notified the Controller thereof.

11. Final provisions

(1) If the property of the Controller which is held by Processor is at risk by actions of third parties (for example by attachment or seizure), by insolvency proceedings or by other events, the Processor shall notify the Controller immediately. A right of retention is excluded with regard to data carriers and data files of the Controller.

(2) The grounds for the Agreement, amendments to the Agreement and ancillary agreements must be in writing, which may also be in an electronic format.

(3) In the event of any conflict between these contractual clauses and the provisions of related agreements existing between the parties or subsequently entered into or concluded, these clauses shall prevail.

(4) Should individual parts of this agreement be invalid, this shall not affect the validity of the remainder of the agreement. In this case, as well as in the case of a gap requiring regulation, the Client and the Contractor shall agree on a solution that comes closest to the economic objective of all parties involved (Client, Contractor, Recipient and affected persons).

Exhibitor

Annex 1

Description of processing

Subject matter of the processing	Deployment of the Scan2Lead application: Operation, maintenance and support of the application software Operation of the Scan2Lead application: Capture and mapping of contact and address data (capture of visitor badge barcode and visitor contact information on business cards.
Nature and purpose of the processing	Deployment of the Application: Data is collected, stored and processed to create and manage access to the Application. Operation of the application: Analysis and matching of data to sort and provide contact and address data for import into the exhibitor's CRM system.
Categories of personal data processed	Deployment of the application: - Name, - First name, - E-mail address. Operation of the application: - Salutation, - title, if applicable, - first name, - last name, - Image, - Company, - function, - phone number, - mobile phone number, - e-mail address, - address, - VAT ID if applicable, - LinkedIn / Xing profile.
Categories of data subjects whose personal data is processed	Deployment of the application: Employees of the client (exhibitor) Operation of the application: Potential and existing customers as well as business partners of the exhibitors
Duration of the processing	The duration of the order results from the duration of the order or the actual use by the client.

Controller's data protection officer	[...]
Processor's data protection officer	datenschutz süd GmbH Wörthstraße 15 97082 Würzburg Tel.: +49 931 30 49 76 0

Annex 2

List of sub-processors used, including processing sites

SUB - PROCESSOR	PROCESSING SITE	DESCRIPTION OF THE PROCESSING	GUARANTEES AGREED WITH THE SUB-PROCESSOR*.
Microsoft Ireland Operations Ltd.	South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin, D 18 P 521, Irland	MS Azure Cloud Services for Data Management and Storage EU	EU Standard Contractual Clauses, Adequacy Decision (EU-U.S. Data Privacy Framework).
ABBYY Europe GmbH	Friedenstraße 22B, 81671 Munich, Germany	Business card recognition module	
ActiveCampaign LLC („Postmark")	1 N Dearborn St FL 5, Chicago, IL 60602, USA	E-mail dispatch (info e-mails to Scan2Lead users)	EU Standard Contractual Clauses, Adequacy Decision (EU-U.S. Data Privacy Framework).
Zoho Corporation Pvt. Ltd.	Beneluxlaan 4B, 3527 HT Utrecht, Niederlande	E-mail dispatch, internal administration, administration of customer data and customer support, invoicing	

*Guarantees may include EU Standard Contractual Clause (SCC), approved Binding Corporate Rules (BCR), or adequacy decision.

Annex 3

Technical and organisational measures according to Article 32 GDPR

Company/ Locations

The following technical and organizational security measures relate to:

- **adventics GmbH**

  Münchener Str. 23A

  85540 Haar near munich, Germany
- **adventics GmbH**

  Seidlgasse 34

  1030 Vienna, Austria

A. Art. 32 GDPR

Taking into account the state of the art, the costs of implementation and the nature, scope, circumstances and purposes of the processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons, adventics GmbH shall implement appropriate technical and organizational measures to ensure a level of protection appropriate to the risk.

B. Measures to ensure confidentiality and integrity

B.1. Access control

Definition

Measures suitable to prevent unauthorized persons from gaining access to data processing systems with which personal data are processed or used.

B.1.1. Office premises

- The office premises of adventics GmbH in Germany are located at Münchner Str.23A, 85540 Haar near Munich.
- The offices of adventics GmbH in Austria are located at Seidlgasse 34, 1030 Vienna.
- The offices are equipped with a mechanical locking system.
- The issuance of keys to employees is recorded.
- The keys are issued by the management.

B.1.2. Visitor regulations

- According to access regulations, visitors are only allowed to move around the office premises if they are accompanied by the responsible contact person at all times.

B.1.3. Access to the server room

- The adventics server rooms on which personal data is processed are located in Europe. The servers are hosted by:
  - Microsoft Azure EU Data Center Europe West/ Netherlands.

The Azure Data Center Europe West has the following certifications: CIS Benchmark | CSA-STAR attestation | CSA-STAR certification | CSA-STAR self-assessment ISO 20000-1:2011 | ISO 22301 | ISO 27001 | ISO 27017 | ISO 27018 | ISO 27701 | ISO 9001 PCI DSS | SOC | WCAG | CDSA | PCI DSS | Shared Assessments | TruSight | BIR 2012 | AFM + DNB NEN-7510D

https://learn.microsoft.com/de-de/azure/security/fundamentals/infrastructure

- Zoho EU Data Center Amsterdam, Netherlands

  The Zoho Data Center in the Netherlands has the following certifications: ISO 27001 ISO 22301 SOC 2 TYPE IIISO 50001 PCI DSSZoho EU Data Center Amsterdam, Niederlande

B.2. access and access control measures

Definition

Measures that ensure that

- data processing systems cannot be used by unauthorized persons,
- attempts to gain unauthorized access do not go unnoticed,
- the persons authorized to use the data processing systems can only access the data subject to their access authorization, and unauthorized reading, copying, modification is prevented,
- the attempt of unauthorized access does not go unnoticed.

B.2.1. Access authorizations

- Defined approval process, which employee has access to which personal data.
- Allocation and access authorizations are logged.
- Each employee receives a personalized user account.
- Each employee must identify himself at each log-in via a 2-factor authentication.
- There is a password parameter:
  - The password contains at least 8 characters,
  - Passwords contain upper and lower case letters, numbers and special characters,
  - Passwords must not be easy to guess (date of birth),
  - Trivial passwords (1111) must not be used,
  - Passwords that have already been used must not be used again.
- The system enforces compliance with the password requirement.
- In case of inactivity, the screen turns off after 5 minutes.
- If compromise is suspected, the password must be changed immediately using 2-factor authentication.
- Login attempts are limited and also remain locked until manually unlocked by IT.
- For remote access, employee identification is also done through 2-factor authentication.
- Login attempts for remote access are limited and also remain blocked until manually cancelled by IT.

B.3. Measures for securing paper documents, mobile data carriers and mobile devices

Definition

Measures that ensure the implementation of appropriate technical and organizational measures also on mobile data carriers and end devices as well as on paper documents.

B.3.1. Paper documents

- Confidential and secret information in paper form shall be disposed of exclusively via the shredder provided in the company (security level P4).

B.3.2. Mobile data carriers and mobile end device

- Data carriers are used for the exchange of data. Data carriers of unknown origin must not be used together with company hardware.
- Mobile data carriers used for data exchange, such as USB sticks, must be encrypted on the hard disk.
- The use of private mobile end devices is prohibited.
- The disposal of mobile end devices and data carriers is carried out by the IT department.

B.3.3. Maßnahmen zur sicheren Datenübertragung

Definition

Measures that ensure that

- Data cannot be read, copied, altered, or removed without authorization during electronic transmission or while being transported or stored on data media.
- Transportation of physical media containing personal data to a document destruction service provider is only carried out in closed containers and in closed vehicles so that no data can be lost.

B.3.4. Forwarding control

- E-mails are transmitted via TLS.
- Operation and use of an FTP server through which file sharing and secure or encrypted file transmission is ensured.
- Data media used for file sharing are encrypted.
- Keys or certificates are managed by in-house IT.

C. Measures to ensure availability

Definition

Measures to secure data (physical / logical) against accidental destruction or loss.

C.1. Server room

- The server room is an interior room without windows.
- The server room is protected by a fire-retardant solid wall access door.
- The server room is connected to the fire alarm control panel.
- The server room is equipped with both an extinguishing system (CO2 extinguisher and halon/ argon extinguishing system) and air conditioning.
- Uninterruptible power supply, which is additionally protected by a diesel generator and its functionality is tested regularly.

C.2. Backup and emergency concept, virus protection

- Documented backup concept.
- Regular testing of the backup concept.
- Execution and documentation of the backup check takes place at regular intervals but at least twice a month.
- The execution and documentation of the backup checks are carried out by the external service providers Microsoft Azure and Zoho.
- The regular creation of backups takes place on the online cloud storage of the aforementioned external service providers.
- The storage of the backups takes place in a separate section from the primary server.

C.2.1.1. Change- und Patchmanagement

- Documentation of change and patch management for which in-house IT is responsible.

C.2.1.2. emergency prevention concept

- Documentation of an emergency preparedness concept with precise action specifications.

C.3. Virus protection

- All servers and clients are provided with virus protection, which is constantly updated by the in-house IT department. As a matter of principle, no computers may be operated without up-to-date virus protection.

C.4. Network connection

- The entire network connection is operated by the in-house IT and is not redundantly connected to each other with regard to the individual locations.

D. Pseudonymization/encryption, Art. 32 (1) a DSGVO

Definition

Pseudonymization (Art. 32 Para. 1 lit. a, Art. 25 Para. 1 DSGVO) ensures that identification features of personal data are replaced by identifiers of specific or identifiable persons, insofar as this is necessary to protect the data subjects or is required from the perspective of data protection law, and therefore the assignment to the data subject is not possible without additional information. Consequently, data can no longer be assigned to a specific data subject without the addition of additional information. This additional information must be stored separately and be subject to appropriate technical and organizational measures.

D.1. Use of pseudonymization

- Where possible, data is processed pseudonymously.
- If data is analyzed as part of the commissioned processing, it is pseudonymized or anonymized in accordance with data protection requirements. Furthermore, pseudonymization of data in the overall process is ensured to the extent that only a unique, usually non-consecutive number is printed or encoded in the 1D or 2D barcode on scannable access badges of visitors and exhibitors ("badges"), which is only merged with the personal data of the respective visitor as part of the encrypted communication of the Scan2Lead front-end devices with the back-end systems.

- Assignment and storage of individual data is done in separate systems from each other.

D.2. Use of encryption

- Where possible, data shall be processed in encrypted form. This is to be assessed on a case-by-case and project-dependent basis.
- - Communication between the frontend devices of Scan2Lead users and the backend systems takes place exclusively using common encryption methods.

E. Procedure for reviewing, assessing and evaluating the measures taken - Art. 32(1)(b), (c), (d) GDPR

E.1. Conducting system audits

- System audits to verify the existing systems and whether they are functioning.
- If deviations or non-conformities are found, these are included in the risk assessment and appropriate countermeasures are initiated.
- Continuous review and documentation of the results.

E.1.1. Data protection management

- Appointment of a company data protection officer
- Commitment to data protection compliance in accordance with the GDPR
- Informing employees on the topics of data protection and data security through training and written explanations (appendix to the declaration of commitment)
- Conducting classroom training and e-learning (e.g., upon hiring) on data protection topics
- Conclusion of contracts for commissioned processing in accordance with Art. 28 DSGVO
- Passing on obligations from the written contract for commissioned processing to subcontractors
- Guidelines and checklists for commissioning service providers
- Control of the technical and organizational measures taken by the contractor
- Informing the client in the event of errors/irregularities in data processing
- Explanations and guidelines on data protection topics and requirements from the GDPR (e.g., dealing with data subject inquiries / procedure in the event of a "data breach," etc.).Bestellung eines betrieblichen Datenschutzbeauftragten

E.1.2. Documentation

- The measures taken are continuously reviewed and revised if necessary.