activeMind.AG

Agreement for the processing of personal data

between

responsible company for the use of the online training (controller)

hereafter: **Controller**

and

activeMind AG
Management- und Technologieberatung
Potsdamer Str. 3

80802 Munich

hereafter: **Processor**

Contents

1 Introduction, scope, definitions

(1) This Agreement defines the rights and obligations of the Controller and Processor (hereafter "Parties") in the context of an agreement for the processing of personal data.

(2) This Agreement contains all applications in which employees or Sub-processors of the Processor process personal data on behalf of the Controller.

This Agreement uses terms corresponding to definitions per the EU General Data Protection Regulation. In this context, the Customer is the "Controller" and the Contractor the "Processor". Any declarations are to be made in writing. Declarations can generally be made in another form as long as it can be verified.

2 Subject and duration of processing

2.1 Subject

The Processor will carry out the following processing activities:

- Set up and maintenance of the online training portal

In carrying out the processing, the Processor can have contact with personal data for which the Controller is responsible.

The processing affects the existing service agreement between the parties (hereafter "Main Agreement").

2.2 Duration

The duration of the service in this Agreement is specified in the Main Agreement.

3 Data processing type, purpose and data subjects

3.1 Type of processing

The type of processing is as follows: Collect, save, read, use, delete

3.2 Purpose of processing

The processing has the following purpose:

Set up and maintenance of a portal of necessary data processing systems in which access to personal data cannot be excluded.

3.3 Type of data

The following data will be processed:

- Surname, first name, email address and user's company
- Course metadata (registration progress and time stamp, learning progress)

3.4 Categories of data subjects

The data subjects are as follows:

- Employees of the Controller

4 Duties of the Processor

(1) The Processor will process personal data exclusively as contractually agreed upon or as instructed by the Controller unless the Processor is legally obligated to carry out specific processing.

(2) The Processor acknowledges all relevant and general data protection regulations. The Processor observes the legal principles of data processing.

(3) Persons who could obtain knowledge of the processing data in connection with this Agreement are obligated in writing to confidentiality and have been made aware of the relevant provisions of data protection and this Agreement.

(4) In connection with processing within this Agreement, the Processor will support the Controller in fulfilling the legal obligations of data protection, especially in preparing and updating records of processing activities, carrying out data protection impact assessments and necessary consultation with supervisory authorities. The Processor is to retain and provide the necessary details and documentation to the Controller immediately upon request.

(5) If the Controller subject to inspection or requests for information from supervisory authorities or other bodies, or if data subjects assert their rights, the Processor shall support the Controller insofar as it involves the processing in this Agreement.

(6) The Processor may provide information to third parties or to data subjects only after prior approval is given by the Controller. The Processor will forward any directly received requests immediately to the Controller.

(7) Processing is to be conducted exclusively within the EU or the European Economic Area.

5 Security of Processing

(1) Taking into account the state of the art, the Processor shall implement appropriate the technical and organisational measures to guarantee that the security of processing is commensurate with the risk, and shall ensure that such security is verifiable at all times and regularly documented. The technical and organisational measures are described in the Appendix to this Agreement. They define the minimum duty of the Processor.

(2) The data security measures can correspond to any advancements in technical and organisational developments as long as they do not fall below the level agreed upon.

(3) The Processor ensures that the processed data related to this agreement will be kept strictly apart from other data.

(4) Copies or duplicates without the knowledge of the controller are not allowed. Technically necessary, temporary duplications are the exceptions as long as the agreed upon level of data protection is not compromised.

(5) The processing of data in private homes is permitted. Insofar as such processing takes place, the Processor shall ensure that a level of data protection and data security corresponding to this Agreement is maintained and that the monitoring rights of the Controller specified in this Agreement can be exercised without restriction in the private homes concerned. Data processing on behalf of the Controller with private devices is not permitted under any circumstances.

(6) The Processor must ensure a process of regular reviews, assessments and evaluations of the effectiveness of technical and organisational measures to ensure the security of processing according to Art. 32 (1)(d) GDPR.

6 Provisions for correcting, deleting and blocking data

(1) The Processor shall rectify, delete or block data processed within the scope of this Agreement only or per the instructions of the Controller.

(2) The Processor shall follow corresponding instructions of the Controller at all times and also beyond the termination of this Agreement.

7 Sub-processing

(1) The Processor shall be entitled to transfer processing operations to a Sub-processor. The Processor will inform the controller of new or replacement Sub-processors.
The Controller may object in writing to an assignment or change for justifiable reasons within two weeks.

(2) Where the Processor engages Sub-processors, the Processor shall be obliged to pass on Processor's contractual obligations hereunder to such sub-processors. Upon request, the Controller shall have access to the relevant contracts between Processor and Sub-processor.

(3) It shall be possible for the Controller to effectively exercise their rights in relation the Sub-processor. In particular, the Controller must be entitled to carry out inspections at any time to the extent specified here, also at Sub-processor, or to have them carried out by third parties.

(4) The Processor's and Sub-processor's responsibilities shall be clearly distinguished.

(5) The current Sub-processors approved by the Controller are indicated in Attachment 2 by name, address and work order content showing the scope of processing of personal data. The other obligations of the Processor to the Sub-processors put forth in this agreement remain unaffected.

(6) Sub-processor relationships in the context of this Agreement are only those services that show a direct connection to the main services being rendered. Ancillary services, such as transportation, maintenance and cleaning as well as the use of telecommunication services or user services are not included. The Processor's obligation to ensure compliance with data protection and data security, even in these cases, remains unaffected.

8 Rights and obligations of the controller

(1) The Controller is solely responsible for the lawfulness of the intended processing, as well as protecting data subjects' rights.

(2) The Processor shall not process any personal data under this Agreement except on the Controller's documented instructions, unless required to do so by Union or Member State law. The Controller can issue verbal instructions in urgent cases. The Controller will immediately confirm such instructions in writing.

(3) The Controller will immediately inform the processor if errors or irregularities are discovered during performance audits.

(4) The Controller or its third party is, to an appropriate extent, authorised to verify compliance with data protection regulations and contractual agreements by the Processor, in particular through obtaining information and inspecting saved data and data processing programs as well as other on-site audits. The Processor is obligated to provide the required information, demonstrate processes and produce evidence that are required during the audit. The Processor is authorised to refuse audits through third parties that are competitors or for other similarly justifiable reasons.

(5) Audits of the Processor shall be carried out without avoidable interruptions of the Processor's business operations. Unless the Controller has justifiable reasons to do so otherwise, audits will take place after sufficient notification, within the business hours of the Processor and not more than every 12 months.

9 Notification duties

(1) The Processor shall notify the Controller without undue delay upon the Processor becoming aware of a Personal Data Breach affecting Company Personal Data, providing the Company with sufficient information to allow the Company to meet any obligations to report or inform Data Subjects of the Personal Data Breach under Data Protection Law.

(2) The Processor shall notify the Controller immediately of any audits or measures by supervisory authorities or other third parties, insofar that there is relevance to this Agreement.

(3) The processor will pledge any necessary support to the Controller in upholding their obligations per Art. 33 and 34 GDPR.

10 Instructions

(1) The Controller reserves the right to provide comprehensive instruction with regard to data processing activities under this Agreement.

(2) The Processor shall immediately inform the Controller if they believe any of the Controller's instructions violates legal requirements. The Processor shall refrain from carrying out that may result in any such infringement until it is confirmed or changed by the Controller’s responsible person responsible for this.

11 Agreement termination

At any time during ongoing cooperation, the Controller can back up the data processed within this Agreement. The Controller is responsible, even possibly after the termination of this Agreement, for promptly backing up or exporting necessary data. The Processor will delete the processed data within two weeks after the termination of this Agreement.

12 Compensation

Processor compensation is arranged within the Main Agreement. There will be no separate compensation or cost reimbursement in the context of this Agreement.

13 Liability

(1) The Controller and Processor are jointly and severally liable for the compensation of damages suffered by a person due to inadmissible or incorrect data processing within the scope of the contractual relationship.

(2) The Controller releases the Processor of initial demands of all third party claims that were raised against the Processor in connection with the processing in the context of this Agreement if damages occurred through the correct implementation of services or through instructions provided by the Controller.

(3) The conditions of liability in the main agreement shall otherwise apply.

14 Miscellaneous

(1) Both parties are obligated to treat as confidential all knowledge of business secrets and data security measures of the other party, within the scope of the contractual relationship, including beyond the termination of the Agreement. If there are doubts as to whether information is subject to confidentiality, that information shall be kept confidential until the other party has given its release in writing.

(2) Should the Controller's assets be jeopardised by the Processor through third party measures (such as seizure or confiscation), through bankruptcy or bankruptcy proceedings, or other events, the Processor must inform the Controller immediately.

(3) Ancillary agreements are to be in writing with express reference to this Agreement.

(4) The objection to the right of retention in terms of § 273 German Civil Code will be excluded regarding the data processing in the context of this Agreement and the associated data media.

(5) If individual terms of this Agreement should become invalid, this will not affect the validity of the remaining parts of this Agreement.

Attachment 1 – Technical and organisational measures

The processor must set up and continually maintain the following technical and organisational measures that have been set to ensure data protection and data security. The aim is to protect confidentiality, integrity and availability of the processed information in the context of this Agreement.

Organisation of information security

The leadership of activeMind AG is responsible for the complete implementation of the principles of IT security in their organisational unit, and for fulfilling their IT security tasks.

Information security roles and responsibilities are defined in the IT security organisation. To reduce the possibilities of unauthorised or unnoticed changes or misuse of company assets, conflicting tasks and areas of responsibility are to be separated.

activeMind AG has a process that dictates when and to which authority known data protection and information security incidents are promptly reported.

Regular contact with special interest groups will be maintained to be informed of changes and improvements in the area of data protection and information security.

Data protection and data security are components of all phases of project methodology.

Data protection and data security will also be guaranteed in the areas of teleworking and mobile device use through the respective guidelines and processes.

Human resource security

Employees were carefully selected for their suitability in their role in the company. Employees' activities are regularly compared with their responsibilities as detailed in their functional descriptions. At the beginning of their employment, all employees sign a confidentiality and data protection agreement that extends beyond the end of their employment. Employees are trained in data protection and data security. Through this training, they are aware of their responsibility.

Protection of personal data and data security are guaranteed through an existing process before, during and after termination of employment. This includes measures in the case of a data breach.

Asset management

All assets (for example equipment, removable storage devices, notebooks) and information that contain personal data are inventoried and managed.

Responsible persons are assigned to protect these assets for the assets' entire life cycle.

There are existing processes for the authorised use of company assets. The return of equipment is carried out in a documented manner.

The information and data are classified and marked according to legal requirements, their value, their criticality and their sensitivity to unauthorised disclosure or changes.

There are existing processes for handling assets, especially removable storage devices, which are developed and implemented in accordance with this classification. There is an existing process that protects data storage devices from unauthorised access, misuse or falsification.

Data storage devices that are no longer in use are disposed of using a documented process and a liable certified service provider.

Access control

There are existing and controlled measures that ensure that persons only have access to personal data for which they are authorised for inspection and processing .

Authorised persons shall get access to IT systems through a monitored process based on an existing and restrictive authorisation plan. Access to networks and network services is controlled and implemented.

Only authorised users have access to systems and services and unauthorised access is inhibited; in particular, there is a formal process in place for user registration and de-registration that assigns access rights.
Administrative rights are limited and monitored.
There is a monitored process in handling passwords. The actual and target states of user access rights are reviewed regularly. These are revoked or adapted as necessary.
Access to data is limited to a need-to-know-basis and access to systems and applications is monitored through a secure registration process. Stronger and more secure passwords are used.
The use of programs that are capable of circumventing system and application protection measures is limited and closely monitored.

Cryptography

Protecting confidentiality, authenticity or integrity of information is ensured through the appropriate and effective use of cryptography. For this purpose, a guideline was implemented for company use of cryptography that includes managing cryptographic keys and that is appropriate for security requirements.

Physical and environmental security

We have adopted controlled measures that are to hinder unauthorised access to data processing systems that are used to process or use personal data. This includes amongst others:

Location Potsdamer Straße 3, 80802 Munich; Location Leopoldstraße 182, 80804 Munich and Location Kurfürstendamm 56, 10707 Berlin

- Building and security areas can only be accessed by authorised persons.
- IT rooms have their own separate security.
- Visitors and suppliers can only enter the building at the main entrance. They may only be admitted by an authorised person. They are escorted by employees within the building.
- No external personnel are assigned in the data centre.
- External persons are to be granted only the necessary minimum access rights.

Operational security

Measures are in place to ensure orderly and secure operations of information and data processing facilities. This includes control in the case of a change to the information processing facilities as well as control and regular measurements of our capacities and resources to ensure availability of required system performance. The above monitoring process is currently in use for the following assets:

- Hard disk status and available memory
- Raid status
- Essential services and status of all virtual machines
- Erroneous log in attempts
- Storage allocation and main storage
- Firewall performance and capacity
- Server accessibility from outside

Data security has a protected process.

Detection, prevention and retrieval measures were adopted as protection from malware and are regularly updated.

The saving of sensitive personal data is recorded with a monitored and protected event log to protect privacy. All logging equipment and information, including administrator and operator logs, are protected from manipulation and unauthorised access.

All company internal clocks are centrally synchronised with a reference clock.

There is a central process for controlling software installations on company systems.

There is a listing of technical assets and the controlled handling of technical vulnerabilities, including patch management with defined responsibilities.

Limits on software installations are centrally regulated.

In the case of an information system audit, measures are in place to keep business process interruptions, as far as possible, to a minimum.

Communication security

As a data protection and security consultancy, the security of personal data and information saved on suitable networks and network services is vital. For this reason, there are existing measures that manage, control and secure networks.
Information services, users and information systems are separated from one another on a need-only basis.
There are guidelines and processes for information and data transfer as well agreements for data transfers to external locations.
Electronic messaging is properly secured. Measures based on the classification system adopted by the organisation protect messages from unauthorised changes.

To protect company internal data, confidentiality and secrecy agreements on a need-only basis are entered into and verified on a regular basis.

System procurement, development and maintenance

Data and information security is a permanent component of the life cycle of suitable systems. This also includes the requirements for and security of information systems that are available through public network services. The need-only basis of applications ensures its secure use. A system change management process was set up to ensure system, application and product integrity from the early design stages to later maintenance work. Business critical applications are checked and tested after changes are made to the operating platforms to verify that there are no negative effects on organisational security, even of customer applications. There is a controlled process to analyse, develop and maintain a secure IT system.

Supplier relationships

Suppliers are carefully pre-selected and checked for their suitability in protecting data and information security.

There are existing processes to ensure protection and secrecy of company internal assets and data. To ensure this protection, suppliers are obligated to adopt technical and organisational measures.

A regimented and user defined access authorisation process is in place for assets and data that are required for each supplier.

Suppliers may contract other suppliers only with the approval of activeMind AG to safeguard a secure supply chain.

Regular data protection and security audits of internal suppliers are carried out to maintain the agreed upon levels. Authorisation assignments are also subject to constant documented control.

Suppliers are obligated to destroy data and assets received from activeMind AG after contract termination. Secrecy protection continues indefinitely.

Handling information security incidents

activeMind AG has an existing controlled process for handling information security and data protection incidents to ensure a consistent and effective approach. Employees are encouraged to immediately report all data protection and security events and are regularly trained for this purpose. A reporting system has been installed for forwarding the event to an intervention team, ensuring a quick response. All events are documented, classified and assessed. The intervention team has precise instructions for dealing with an event.
Improvement measures that emerge from the knowledge and evidence collected from an event are regularly discussed and implemented together with management.

Information security aspects in business continuity management

In the context of information security, system availability is specifically assessed and documented. Technical and organisational specifications, such as redundant systems / connections or the associated planning, are derived from the requirements and are implemented consistently and in a controlled manner. An overall emergency plan provides the framework for handling select scenarios. Continuously updated plans for testing adopted measures and existing testing processes complete the overall emergency management.

Compliance

All relevant legal, regulatory, self-imposed or contractual requirements as well as our company's approach for complying with these requirements are defined, documented and kept up to date.

Appropriate processes were also implemented to ensure compliance with legal, regulatory, and contractual requirements regarding intellectual property and the use of copyright protected software products.

We protect the logging of personal data on a need-only basis according to legal, regulatory, contractual and business requirements.

Controls of cryptographic measures are considered.

To ensure protection of information and data, a regular independent audit is carried out of the company's internal information security and data protection level, security and data protection guidelines as well as compliance with technical specifications.

Attachment 2 – Approved sub-processors

Company	Address	Contents of agreement
Global Access Internet Services GmbH	Potsdamer Straße 3, 80802 Munich	ISO 27001-certified data centre
Midland-IT GmbH	Marienstraße 76, 32427 Minden	IT-Support
neudenken Strategieagentur	Friedrichstraße 123, 10117 Berlin	Technical website design and administration services
JKDV-Systeme GmbH	Bahnstraße 34, 25451 Quickborn	Technical website design and administration services

Attachment 3 – Persons with authority to issue instructions, addresses for reporting data protection violations

The following persons are authorised to give and receive instructions:

- Klaus Foitzick, activeMind AG
- Michael Plankemann, activeMind AG
- Dr. Evelyne Sørensen, activeMind AG

Attachment 4 – Data protection officer

At this time, the processor's data protection officer is internal:

Data protection officer of activeMind AG
Telephone: +49 (0)89 / 91 92 94 - 900
email: datenschutz@activemind.de

Attachment 5 – Certificates

TÜV PROFI CERT

CERTIFICATE

Management system as per

ISO/IEC 27001:2013

Evidence of conformity with the above standard(s) has been furnished and is certified in accordance with TÜV PROFICERT procedures for

ActiveMind AG Management- und Technologieberatung
Potsdamer Str. 3, 80802 München / Germany

with the location:

activeMind.AG

activeMind AG Management- und Technologieberatung
Potsdamer Straße 3
80802 München / Germany

scope:

Designation of data protection officers, information security officers.
Installing and auditing of privacy- and information-security management systems;
hosting and management of customer portals

Statement of Applicability (SoA): Version 4 / 2019-02-04

Certificate registration No. **73 121 6356-1** Certificate valid from 2019-06-27 to **2022-06-26**

Audit report No. 4348 9948

DAkkS Deutsche Akkreditierungsstelle D-ZM 14137-01-00

TÜV HESSEN

Darmstadt, 2019-06-27
Certification body of TÜV Hessen
– Head of Certification body –

PAGE 3. Only valid in conjunction with the main certificate 73 121 6356.
This certification was conducted in accordance with the TÜV PROFICERT auditing and certification procedures and is subject to regular surveillance audits. Verifiable under www.proficert.com. Original certificates contain a glued on hologram.
TÜV Technische Überwachung Hessen GmbH, Robert-Bosch-Straße 16, D-64293 Darmstadt, Tel. +49 6151/600331 Rev-GB-1711

TÜV PROFI CERT

CERTIFICATE

Management system as per

DIN EN ISO 9001:2015

Evidence of conformity with the above standard(s) has been furnished
and is certified in accordance with TÜV PROFiCERT procedures for

ActiveMind AG Management- und Technologieberatung
Potsdamer Str. 3, 80802 München / Germany

with the location:

activeMind.AG

activeMind AG Management- und Technologieberatung
Potsdamer Straße 3
80802 München / Germany

scope:

Designation of data protection officers, information security officers.
Installing and auditing of privacy- and information-security management systems;
hosting and management of customer portals

Certificate registration No. **73 100 6356-1** Certificate valid from 2019-05-02 to **2022-05-01**

Audit report No. 4348 9948

DAkkS Deutsche Akkreditierungsstelle D-ZM-14137-01-00

TÜV HESSEN

Darmstadt, 2019-05-02
Certification body of TÜV Hessen
– Head of Certification body –

PAGE 3. Only valid in conjunction with the main certificate 73 100 6356.
This certification was conducted in accordance with the TÜV PROFICERT auditing and certification procedures and is subject to regular surveillance audits. Verifiable under www.proficert.com. Original certificates contain a glued on hologram.
TÜV Technische Überwachung Hessen GmbH, Robert-Bosch-Straße 16, D-64293 Darmstadt, Tel. +49 6151/600331 Rev-GB-1711