MAXQDA AI Add-On: General Terms and Conditions (GTC) for Universities, Research Institutions, Companies

Date revised last: April 2023

The VERBI Consult. Software. Sozialforschung GmbH ("VERBI") currently develops the MAXQDA AI Add-On, an addition to the standard software "MAXQDA". The MAXQDA AI Add-On allows the customer to automatically summarise texts (documents, coded segments or memos). Currently, only a beta version of the MAXQDA AI Add-On is available. VERBI offers customers the opportunity to register as a tester for the beta version of MAXQDA AI Add-On in order to test the functionality and usability of MAXQDA AI Add-On free of charge. The use of the beta version of MAXQDA AI Add-On is subject to the following conditions of use.

For the use of the standard software "MAXQDA" separate GTC/EULA apply. Furthermore, the GTC/EULA for the standard software "MAXQDA" also apply to the use of the MAXQDA AI Add-On, unless these GTC/EULA include more specific provisions.

§ 1 General Information concerning the Beta Version

1. The MAXQDA AI Add-On is a beta version, i.e. a pre-release and not final version of the feature. The beta version has not yet been exhaustively tested and may therefore be incomplete and/or include errors and inaccuracies. VERBI therefore does not guarantee for a particular condition, quality or availability of the beta version of MAXQDA AI Add-On.

2. The provision of the beta version of MAXQDA AI Add-On is based on availability and is subject to continuous change and optimisation. This means that VERBI may, at any time, adjust, restrict or completely discontinue the use of the beta version of MAXQDA AI Add-On for the customer (even without providing reasons). The customer cannot derive any claims against VERBI from a change, restriction or discontinuation of the beta version of MAXQDA AI Add-On.

3. The use of the standard software "MAXQDA" remains unaffected by any restrictions on the use of the beta version of MAXQDA AI Add-On.

§ 2 User Registration

1. To use the beta version of MAXQDA AI Add-On, customers must register as a tester on our website. The use of the beta version of MAXQDA AI Add-On comes free of charge for the customer.

2. Registration as a tester requires the existence or conclusion of a paid user contract (subscription) for the MAXQDA standard software. The existence or conclusion of a free demo license will not be sufficient.

3. When completing the registration process, customers already in possession of a paid usage

contract for the MAXQDA standard software will receive a key to unlock the beta version of the MAXQDA AI Add-On. Enabling the beta version can be done within the MAXQDA account. If necessary, such an account must be created first. New customers can register as a tester for the beta version of the MAXQDA AI Add-On when signing a contract for the MAXQDA standard software by adding the MAXQDA AI Add-On to their booking.

§ 3 Subject Matter of the MAXQDA AI Add-On Beta Version

1. The beta version of MAXQDA AI Add-On allows the customer to summarise texts automatically. For this purpose, the customer submits the relevant texts to VERBI by using an interface to the MAXQDA AI Add-On beta version.

2. The automated aggregation of texts will not be performed by VERBI, but by OpenAI, L.L.C. ("OpenAI"). For summarising, OpenAI uses artificial intelligence or machine learning. Artificial intelligence and machine learning are based on probabilities. As a result, the use of artificial intelligence and machine learning may produce erroneous results. Meaning that summaries of the customer's texts, generated by OpenAI, may not be correct under all circumstances. The customer understands the possible limitations in reliability.

3. If necessary, VERBI will prepare and/or revise the texts provided by the customer for the summary performed by OpenAI. Corresponding preparations and/or post-processings refer exclusively to formal adjustments of the texts (e.g. splitting if texts exceed the length permitted by OpenAI). VERBI has no influence on summaries created by OpenAI. In particular, VERBI does not review the content of the summary before passing it on to the customer.

§ 4 Scope and Limitations of Use

1. The customer's scope of use of the MAXQDA AI Add-On beta version is limited. Users can view their daily volume available directly in MAXQDA.

2. Furthermore, the customer is not permitted to use the MAXQDA AI Add-On beta version in a manner that violates laws or rights of third parties or that unlawfully affects their rights or otherwise violates the provisions of these GTC or the terms of use of OpenAI (as amended from time to time, available online at https://openai.com/policies/usage-policies). In particular, the use of the function for the following purposes or the provision of the following content is prohibited:

- Illegal activities;
- Content concerning sexual abuse of children or content that exploits or harms children;
- Generating hate, harassment or violent content.
- Generating malware
- Activities that pose a high risk of physical harm, including the development of weapons, military and warfare activities, the management or operation of critical infrastructures with regard to energy, transportation, and water
- Content that incites, encourages or depicts self-harming acts such as suicide, cutting and eating disorders
- Activities that pose a high risk of economic harm, including multi-level marketing, gambling,

lending, automated eligibility decisions concerning loans, jobs, educational institutions, or public assistance services;
- Fraudulent or deceptive activities;
- Adult content, adult industries, and dating apps, including pornography;
- Political campaigning or lobbying;
- Activities that violate the privacy of individuals;
- Unauthorised practice of the legal profession or offering customized legal advice without a qualified person reviewing the information;
- Tailored financial advice without a qualified person reviewing the information;
- Providing information indicating that one has or does not have a particular health condition or providing instructions on how to cure or treat a health condition;
- Government decisions.

3. The customer is also not permitted

- to claim that the summary was generated by humans, although not the case.

4. The publication and sharing of the summary generated by OpenAI is subject to OpenAI's Sharing and publication policy (as amended from time to time, available online at https://openai.com/policies/sharing-publication-policy).

§ 5 Data Protection

1. Data Processing Agreement

1.1 Annex 1 to these GTC contains the VERBI Data Processing Agreement ("DPA"). This DPA constitutes the mutual agreement of the parties with respect to the processing of personal data by VERBI when the Customer uses the beta version of MAXQDA AI Add-On in accordance with these GTC.

1.2 The DPA forms an integral part of the GTC. Upon the Customer's consent to these GTC, the DPA shall also become effective between the parties.

1.3 In the event of any conflict or inconsistency between the DPA and these GTC, the DPA shall prevail to the extent of such conflict or inconsistency.

2. Standard Contractual Clauses

2.1 If the Customer is located in a country outside the European Economic Area for which the European Commission has not issued an adequacy decision, the Customer's use of the beta version of MAXQDA AI Add-On pursuant to these GTC is further governed by Annex 2.

2.2 Annex 2 to these GTC contains the Standard Contractual Clauses of the European Commission in the form of Module 4 (Transfer from a Processor to a Controller) ("SCC").

2.3 The SCC form an integral part of the GTC. Upon the Customer's consent to these GTC, the SCC shall also become effective between the Parties.

3. Definitions

Terms not otherwise defined in the DPA and/or the SCC shall have the meaning set out in the GDPR.

§ 6 Duration of Use

1. The MAXQDA AI Add-On is a beta version. VERBI is entitled to restrict or terminate the customer's use of the beta version of MAXQDA AI Add-On at any time.

2. Furthermore, the customer may terminate the testing of the beta version of MAXQDA AI Add-On at any time.

3. The customer's use of the beta version of MAXQDA AI Add-On will end in any case upon termination of the customer's user contract for the use of the standard software "MAXQDA".

4. After terminating the use, the access to the beta version of MAXQDA AI Add-On will be blocked for the customer.

§ 7 Liability

1. VERBI is liable without limitation for intent and gross negligence. VERBI shall also be liable for slight negligence in the event of damage resulting from injury to body, life or health in accordance with the statutory requirements. In other cases of slight negligence, VERBI is only liable in the event of a breach of such obligations that make the reasonable and proper performance of the contract possible in the first place and on the fulfilment of which the Customer accordingly relies and may rely (cardinal obligations) and only limited to compensation for the foreseeable, typically occurring damage. Furthermore, limitations and exclusions in this clause do not apply to claims by the Customer in the event of fraudulent concealment of a defect by VERBI due to the absence of an assured characteristic, the breach of warranty promise and claims in accordance with §§ 1, 4 of the Product Liability Act (*Produkthaftungsgesetz*).

2. Summaries of customer texts, created using the beta version of MAXQDA AI Add-On, are provided free of charge and by integrating a third-party service from OpenAI. VERBI does not have any influence on this service and is, in particular, not liable for its accuracy, completeness and/or reliability.

3. Any further liability, irrespective of the legal basis, is excluded.

Annex 1

Commission Implementation decision (EU) 2021/95 of 4 June 2021 on standard contractual clauses between controllers and processors under Art. 28 (7) GDPR

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5

Docking Clause

[intentionally left blank]

A SECTION II - OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7

Obligations of the Parties

7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). 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 and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. 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.

7.5. Sensitive Data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6. Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

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

7.7. Use of sub-processors

(a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least five business days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall

provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) 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 contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) 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.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) 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. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions.

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8 (b), 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:

(1) 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') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) 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 obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 of Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay;

(c) in complying, pursuant to Article 34 of Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay. The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III – FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I – LIST OF PARTIES

Controller:

The controller is the customer in accordance with the General Terms & Conditions (GTC) and End User License Agreement (EULA) of VERBI Software. Consult. Sozialforschung GmbH.

Signature and accession date: Effective with agreement to the General Terms & Conditions (GTC) by the customer.

Processor:

Name: VERBI Software. Consult. Sozialforschung GmbH

Address: Invalidenstr. 74, 10557 Berlin

Contact person's name, position and contact details: The data protection officer of VERBI GmbH can be reached at kontakt@datenschutzrechte.de.

Signature and accession date: Effective with agreement to the General Terms & Conditions (GTC) by the customer.

ANNEX II – DESCRIPTION OF THE PROCESSING

Categories of data subjects whose personal data is processed

All individuals whose personal data are contained within the texts provided by the customer in the beta version of MAXQDA AI Add-On.

Categories of personal data processed

All data contained in the texts provided by the customer in the beta version of MAXQDA AI Add-On.

Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

No sensitive personal data is intended to be processed. If a text of the Customer contains corresponding sensitive data, the Customer will pseudonymize or anonymize this data before uploading the project in the beta version of MAXQDA AI Add-On, provided that the pseudonymization or anonymization of the data does not prevent the fulfilment of the processing purpose.

Nature of the processing

Automated text summarisation using artificial intelligence and machine learning.

Purpose(s) for which the personal data is processed on behalf of the controller

Automated text summarisation using artificial intelligence and machine learning.

Duration of the processing

Once the data provided by the customer in the beta version of MAXQDA AI Add-On is no longer required for processing, it will be deleted immediately, although no later than after 30 days.

For processing by (sub-) processors, also specify subject matter, nature and duration of the processing.

When using the beta version of MAXQDA AI Add-On, data is stored on an AWS cloud server and transferred to OpenAI. The processing helps to prepare the texts for summarisation as well as for the summarisation by OpenAI. In turn, the data will be deleted immediately after the need for processing ceases to exist, but at the latest after 30 days.

ANNEX III - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational security measures implemented by the processor(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons. Examples of possible measures:

1. Measures for the security of processing (Art. 32 para. 1 GDPR)

1.1 Access control

Measures suitable for preventing unauthorised persons from gaining access to data processing systems with which personal data are processed or used.

- Alarm system
- Security locks
- Locking system with code card
- Bell system with camera
- Visitors' book
- Care in the selection of security staff
- Care in the selection of the cleaning service

1.2 Access control

Measures suitable for preventing data processing systems (computers) from being used by unauthorised persons.

- Login with user name + password
- Use of anti-virus software
- Use of firewall software
- Use of VPN for remote access
- Creation of user profiles
- Assignment/administration of user authorisations
- Allocation of passwords
- Guidelines for: "Secure password" and "Delete/Destroy"

1.3 Access control

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

- Use of shredders
- Physical erasure of data media
- Proper destruction of data media (DIN 32757)
- Logging of access to applications, specifically when entering, changing and deleting data

- Administration of rights by system administrator
- Number of administrators reduced to the "bare minimum"

1.4 Segregation control

Measures to ensure that data collected for different purposes can be processed separately.

- Separation of development and test environment
- Strictly separate storage of data in different client systems
- Providing data records with purpose attributes/data fields
- Determination of database rights
- Control via authorisation concept

1.5 Pseudonymisation

The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that this additional information is kept separately and is subject to appropriate technical and organisational measures:

- Internal instruction to anonymise / pseudonymise personal data where possible in the event of disclosure.

2. Procedures for regular review, assessment and evaluation (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

2.1 Data Protection measures

- Software solutions for data protection management in use
- Central documentation of all procedures and regulations on data protection with access for employees as required / authorised on the intranet
- Regular review of the effectiveness of the technical protection measures
- Appointment of an external data protection officer (Sebastian Dramburg; kontakt@datenschutzrechte.de)
- Staff training: trained and committed to confidentiality/data secrecy
- Data protection impact assessment is carried out as required
- VERBI GmbH complies with the information obligations according to Art. 13 and 14 GDPR
- Formalised process for processing requests for information from data subjects is in place.

2.2 Incident response management

Support in responding to security breaches

- Documentation of security incidents and data breaches, e.g. via the ticket system.

- All employees are instructed and trained to ensure that data protection incidents are recognised and reported immediately to the DPO.

2.3 Order control (outsourcing to third parties)

Measures to ensure that personal data processed on behalf of the client can only be processed in accordance with the client's instructions.

- Selection of the contractor under due diligence aspects (in particular with regard to information security).
- Regular monitoring of contractors
- The principle of necessity and data minimisation is taken into account.
- The necessary agreements on commissioned processing or EU standard contractual clauses are concluded.

Description of the specific technical and organisational measures to be taken by the processor to be able to provide assistance to the controller:

The current version of the AWS Security Standards (Annex 1 to the AWS DPA) apply.

Anlage 2

Commission implementing decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council

Standard Contractual Clauses

MODULE FOUR: Transfer processor to controller

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)1 for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer"),

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1 (b) and Clause 8.3(b);

(iii) [intentionally left blank];

(iv) [intentionally left blank];

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking Clause

[intentionally left blank]

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data7, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9

Use of sub-processors

[intentionally left blank]

Clause 10

Data subject rights

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13

Supervision

[intentionally left blank]

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

[intentionally left blank]

Clause 15

Obligations of the data importer in case of access by public authorities

[intentionally left blank]

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679

becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Germany.

Clause 18

Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the courts of Germany.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

Data exporter:

Name: VERBI Software. Consult. Sozialforschung GmbH

Address: Invalidenstr. 74, 10557 Berli

Contact person's name, position and contact details: The data protection officer of VERBI GmbH can be reached at kontakt@datenschutzrechte.de.

Activities relevant to the data transferred under these Clauses: Provision of beta version of MAXQDA AI Add-On

Signature and date: Effective with agreement to the General Terms & Conditions and End User License Agreement (EULA) by the customer.

Role (controller/processor): Processor

Data importer:

The controller is the customer in accordance with the General Terms & Conditions (GTC) and End User License Agreement (EULA) of VERBI Software. Consult. Sozialforschung GmbH.

Activities relevant to the data transferred under these Clauses: Provision of beta version MAXQDA AI Add-On

Signature and date: Effective with agreement to the General Terms & Conditions (GTC) and End User License Agreement (EULA) by the customer.

Role (controller/processor): Controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

All individuals whose personal data are contained within the texts provided by the customer in the beta version of MAXQDA AI Add-On.

Categories of personal data processed

All data contained in the texts provided by the customer in the beta version of MAXQDA AI Add-On.

Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

No sensitive personal data is intended to be processed. If a text of the Customer contains corresponding sensitive data, the Customer will pseudonymize or anonymize this data before uploading the project in the beta version of MAXQDA AI Add-On, provided that the pseudonymization or anonymization of the data does not prevent the fulfilment of the processing purpose.

The frequency of the transfer (eg. whether the data is transferred on a one-off or continuous basis)

Continuous transfers during the customer's use of the beta version of MAXQDA AI Add-On.

Nature of the processing

Automated text summarisation using artificial intelligence and machine learning.

Purpose(s) of the data transfer and further processing

Automated text summarisation using artificial intelligence and machine learning.

Duration of the processing

Once the data provided by the customer in the beta version of MAXQDA AI Add-On is no longer required for processing, it will be deleted immediately, although no later than after 30 days.

For processing by (sub-) processors, also specify subject matter, nature and duration of the processing.

When using the beta version of MAXQDA AI Add-On, data is stored on an AWS cloud server and transferred to OpenAI. The processing helps to prepare the texts for summarisation as well as for the summarisation by OpenAI. In turn, the data will be deleted immediately after the need for processing ceases to exist, although no later than after 30 days.