Last update: March 2025

The VERBI Consult. Software. Sozialforschung GmbH ("**VERBI**") offers its customers the possibility to extend the standard software "MAXQDA" with additional functions (such as **MAXQDA AI Assist**) or to use the **MAXQDA TeamCloud** in addition to the standard software (hereinafter collectively referred to as "**Add-Ons**").

General Part

§ 1 Scope of application

1. the separate GTC/EULA apply to the use of the "MAXQDA" standard software. Furthermore, the GTC/EULA for the standard software "MAXQDA" also apply to the use of the add-ons, unless the GTC below contain more specific provisions.

2 In the event of a contradiction between the general part of these GTC, GTC/EULA for the standard software "MAXQDA" and the GTC for the MAXQDA Add-Ons, the following priority relationship applies:

1. specific GTC for the individual Add-Ons as part of these GTC,
2. General part of these GTC,
3. the GTC/EULA for the standard software "MAXQDA".

§ 2 Conclusion of contract

The provisions in the GTC/EULA for the standard software "MAXQDA" apply accordingly to the conclusion of the contract for the add-ons, unless these GTC contain deviating provisions.

§ 3 Prices and terms of payment

The prices stated by VERBI at the time of purchasing apply to the use of the Add-Ons. Furthermore, the provisions in the GTC/EULA for the MAXQDA standard software regarding prices and payment terms for the add-ons apply accordingly.

§ 4 Requirements for the use of Add-ons

The requirement for the use of the Add-Ons is the existence of a paid subscription by the customer for the use of the standard MAXQDA software in accordance with the provisions of the GTC/EULA for the standard MAXQDA software. The details can be found in the corresponding section of these GTC for the respective add-on.

§ 5 Data Protection

§ 5 does not apply if the customer is a natural person and the processing of personal data is carried out exclusively for personal or family research.

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 Add-Ons are used by the Client in accordance with these GTC.

1.2 The DPA forms an integral part of the GTC. Upon the client'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 the GTC, the DPA shall prevail to the extent that such conflict or inconsistency exists.

2. Standard contractual clauses

2.1 If the Customer is located in a country outside German speaking countries of Europe (DACH) for which the European Commission has not issued an adequacy decision, **Annex 2** shall also apply to the Customer's use of the Add-Ons in accordance with the GTC.

2.2 **Annex 2** to these GTC/EULA contains the Standard Contractual Clauses of the European Commission in the form of Module 4 (Transmission 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 given to them in the GDPR.

§ 6 Liability

1. VERBI shall be liable without limitation for intent and gross negligence. VERBI shall also be liable for slight negligence in the event of injury to body, life or health in accordance with the statutory provisions. In other cases of slight negligence, VERBI shall only be liable in the event of a breach of such obligations that are essential for the appropriate and proper performance of the contract and on the fulfillment of which the customer relies and may rely accordingly (cardinal obligations) and only limited to compensation for foreseeable, typically occurring damage. Furthermore, limitations and exclusions in this clause do not apply to claims of the customer in the event of fraudulent concealment of a defect by VERBI, due to the absence of a

warranted characteristic, the breach of a guarantee promise and claims under §§ 1, 4 of the Product Liability Act.

2. Liability is otherwise excluded, regardless of the legal grounds.

§ 7 Withdrawal Policy

§ 7 only applies if the customer acts as a consumer (§ 13 BGB).

1. Right of withdrawal

1.1 You have the right to withdraw from this contract within fourteen days without giving any reason. The withdrawal period lasts fourteen days from the date of conclusion of the contract.

1.2 To exercise your right of withdrawal, you must inform us (VERBI Software. Consult. Sozialforschung GmbH, Invalidenstr. 74, 10557 Berlin, Tel.: +49 (0)30 206 22 5922, Fax: +49 (0)30 206 22 59 29, E-Mail: cs@maxqda.com) of your decision to withdraw from this contract by an unequivocal statement (e.g. a letter sent by post or e-mail). You can use the attached sample withdrawal form, but this is not mandatory.

1.3 In order to comply with the withdrawal period, it is sufficient for you to send the notification of the exercise of the right of withdrawal before the expiry of the withdrawal period.

2. Effects of withdrawal

2.1 If you withdraw from this contract, we shall reimburse to you all payments received from you, including the costs of delivery (with the exception of the supplementary costs resulting from your choice of a type of delivery other than the least expensive type of standard delivery offered by us), without undue delay and in any event not later than 14 days from the day on which we are informed about your decision to withdraw from this contract. For this repayment, we will use the same means of payment that you used for the original transaction, unless expressly agreed otherwise with you; under no circumstances will you be charged any fees for this repayment.

2.2 You will only be liable for any diminished value of the goods resulting from the handling other than what is necessary to establish the nature, characteristics and functioning of the goods.

3. Important note

Pursuant to Section 356 (5) BGB, the right to cancel a contract for the delivery of digital content that is not on a physical data carrier (e.g. software purchased via download) expires when

1. VERBI has commenced the performance of the contract,

2. the consumer has explicitly consented to VERBI commencing performance of the contract before expiry of the withdrawal period,

3. the consumer has confirmed his knowledge that he loses his right of withdrawal by consenting to the commencement of the performance of the contract, and

4. VERBI has provided the consumer with confirmation of the contract.

VERBI shall commence performance of the contract as described above at the time the consumer starts the download process.

4. Model withdrawal form

(Complete and return this form only if you wish to withdraw from the contract).

> To VERBI Software. Consult. Sozialforschung GmbH Invalidenstr. 74 10557 Berlin e-mail: cs@maxqda.com:
>
> I/We (*) hereby give notice that I/We (*) withdraw from my/our (*) contract of sale of the following goods (*)/for the provision of the following service (*),
>
> Ordered on (*)/received on (*),
>
> Name of consumer(s),
>
> Address of consumer(s),
>
> Signature of consumer(s) (only if this form is notified on paper),
>
> Date
>
> (*) Delete as applicable

§ 8 Governing Law and Language

These Terms and Conditions are governed by the laws of the Federal Republic of Germany. The English translation is provided for convenience; in case of discrepancies or ambiguities, the German version shall prevail.

AI Assist

This section only applies to customers who have concluded a contract with VERBI for the use of MAXQDA AI Assist in addition to the use of the standard software "MAXQDA".

AI Assist is a virtual research assistant. AI Assist contains various functions that supplement the standard "MAXQDA" software. Among other things, AI Assist offers the customer the option of text editing and analysis as well as transcription. The use of AI Assist is subject to the following specific terms of use:

§ 1 Subject matter of the contract

1. The subject matter of the contract is the use of AI Assist.

2. AI Assist consists of different modules (see § 3).

3. VERBI offers AI Assist in two options:

- **AI Assist (free)**
- **AI Assist (premium)**

The options differ in the respective available volume of the individual modules of AI Assist.

§ 2 Ordering AI Assist

1. A concluded contract (subscription) for the standard software MAXQDA is required for the use of AI Assist (premium). The existence or use of a free demo license is not sufficient.

2. AI Assist (free) is available to all customers. The existence of a free demo license is the minimum requirement for AI Assist (free)

3. AI Assist and MAXQDA Transcription can be added by the customer through our online shop. Afterwards, AI Assist is visible to the customer in MAXQDA. Before using AI Assist for the first time, the customer must create a MAXQDA account in MAXQDA if no such account already exists.

§ 3 Subject matter of AI Assist

1. General

1.1 The functions of AI Assist are based on software solutions using artificial intelligence. Artificial intelligence is based on probabilities. This can lead to incorrect results when using artificial intelligence. This means that the results generated using artificial intelligence may not be correct in all cases. The customer is aware of the possible limitations on reliability in relation to the use

of AI Assist.

1.2 VERBI uses various third-party services from external service providers for the individual functions of AI Assist. If necessary, VERBI prepares and/or post-processes the files provided by the client before forwarding them to the respective service provider. Such preparation/post-processing relates exclusively to formal adjustments (e.g. splitting if the file exceeds the permitted length). VERBI has no influence on the results produced by the service provider. VERBI does not check the content of the results before forwarding them to the customer.

2. Data analysis with integration of AI

2.1 Data analysis with the integration of AI offers the customer a wide range of options for text processing and analysis. This includes, for example, automatically summarizing and/or paraphrasing texts. The customer can also perform analyzes to generate code suggestions or code text passages directly.

2.2 The data analysis of the customers data with integration AI is not carried out by VERBI itself, but by service providers used by VERBI. The service providers use artificial intelligence for data analysis. A regularly updated list of the service providers used can be found here: https://www.maxqda.com/subprocessors. There is no entitlement to the use of a specific service provider or a specific method of artificial intelligence. The service providers used can be changed at any time if this does not result in any changes to the use of data analysis with the integration of AI. If the change of service provider involves changes to the data analysis, the change will only be made if there is a valid reason for it. A valid reason for a change exists if the software is to be improved, an adaptation to new technical conditions is necessary, a uniform upgrade is required to avoid several parallel versions, or other important operational reasons make the change necessary.

3. Tailwind

3.1 In addition to data analysis with AI integration, VERBI offers the AI App, a web application that is currently in the beta phase and thus available in beta version.

3.2 The functions of Tailwind are diverse. The customer uploads text documents, which are then automatically summarized and analyzed according to various criteria. For example, Tailwind offers functions such as the creation of summaries of individual documents and the recognition of relevant topics that occur in several documents.

3.3 All data processing takes place in the cloud and the results can be exported by the customer.

3.4 AI App is included as a function in AI Assist during the beta phase. During the beta phase, use is free of charge. However, we reserve the right to discontinue the operation of the app after the end of the beta phase, to restrict access or to charge for its use.

3.5 The summaries in Tailwind are not carried out by VERBI itself, but by service providers used by VERBI. The service providers use artificial intelligence for data analysis. A regularly updated list of the service providers used can be found here: https://www.maxqda.com/subprocessors. There is no entitlement to the use of a specific service provider or a specific method of artificial intelligence. The service providers used can be changed at any time if this does not result in any changes to the AI app. If the change of service provider involves changes to the AI app, the change will only be made if there is a valid reason for it. A valid reason for a change exists in particular if the software is to be improved, an adaptation to new technical conditions is necessary, a uniform upgrade is required to avoid several parallel versions, or other important operational reasons make the change necessary.

4. MAXQDA Transcription

4.1 In addition to manual transcription, MAXQDA Transcription offers the customer the option of having audio files transcribed automatically. To do this, the customer imports the audio file into MAXQDA and selects the "Transcribe" option. In this case, a transcript is created by a service provider via an interface (see 3.2), which is automatically imported into MAXQDA. Alternatively, the customer uploads the audio file to the MAXQDA Account web interface and VERBI forwards it to a service provider. The client can download the created transcript from the MAXQDA Account website and then import it into MAXQDA. The client also has the option of entering parameters for the transcription (e.g. regarding language or technical terms).

4.2 The automated transcription of the client's audio file is not carried out by VERBI itself, but by service providers used by VERBI. The service providers use artificial intelligence for the transcription. A regularly updated list of the service providers used can be found here: https://www.maxqda.com/subprocessors. There is no claim to the use of a specific service provider or a specific method of artificial intelligence. The service providers used can be changed at any time if this does not result in any changes to the use of MAXQDA Transcription. If the change of service provider is associated with changes to MAXQDA Transcription, the change will only be made if there is a valid reason for it. A valid reason for a change exists if the software is to be improved, an adaptation to new technical conditions is necessary, a uniform upgrade is required to avoid several parallel versions, or other important operational reasons make the change necessary.

4.3 MAXQDA Transcription is not automatically included in AI Assist but can be additionally purchased through our online shop.

§ 4 Scope and limitation of use

1. The scope of use of AI Assist is limited for each customer. Should unusually high or automated usage patterns occur, we reserve the right to control the processing capacity accordingly.

2. The customer is not permitted to use AI Assist in a way that violates the law or the rights of third parties or unlawfully affects their rights or otherwise violates the provisions of the GTC or those of the service providers (in the current version). In particular, the use of AI Assist for the following purposes or for distributing the following content is prohibited:

- Illegal activities;
- Content about child sexual abuse or content that exploits or harms children;
- Content on or activities promoting the development or distribution of illegal substances, goods or services;
- Creation of discriminatory content or hate, harassment or violence content;
- Malware generation;
- Activities that pose a high risk of physical harm, including weapons development, military and war activities, management or operation of critical energy, transport and water infrastructures;
- Content that incites, encourages or depicts self-harming acts such as suicide, cutting and eating disorders;
- Activities that carry a high risk of economic harm, including multi-level marketing, gambling, lending, automated eligibility decisions, employment, education or public assistance services;
- Activities that impair or circumvent the security or security measures of a service or system or impair their agreed or intended use;
- Fraudulent or deceptive activities;
- Adult content, adult industries and dating apps, including pornography;
- Political campaigning or lobbying;
- Activities that violate the privacy or property of individuals;
- Activities that may cause environmental damage;
- Unauthorized practice of law or offering tailored legal advice without a qualified person having reviewed the information;
- Tailored financial advice without verification of information by a qualified person;
- Providing information that he or she has or does not have a particular health condition or giving instructions on how to cure or treat a health condition;
- Government decisions.

3. The terms of use of the respective service providers are linked on our website under the respective service providers used: https://www.maxqda.com/subprocessors.

4. The customer is also not permitted,

- to claim that the result generated with the help of AI Assist was produced by humans,

although this is not the case.

5. The customer is not permitted to edit, modify or change the software (in whole or in part) or to disassemble, decompile, reverse engineer or convert the software in whole or in part, nor may the customer permit or enable third parties to do so. Furthermore, the customer may not use the software to create, train or improve a similar or competing product or service (directly or indirectly).

§ 5 Term and termination of contract

1. The use of AI Assist by the customer ends in any case with the termination of the customer's contract for the use of the standard software "MAXQDA".

2. After termination of use, access to AI Assist will be blocked for the customer.

§ 6 Liability

The results produced by AI Assist are done through the integration of third-party services. VERBI has no influence on this performance and is not liable for its accuracy, completeness and/or reliability.

§ 7 Data protection

§ Section 7 shall not apply insofar as the customer is a natural person and the processing of personal data is carried out during a purely personal or household activity.

1. Data analysis with integration of AI and AI app

1.1 The following information contains the relevant information for Attachment II of the DPA (see General Part § 5 No. 1 and **Annex 1**) and Attachment I Section B of the SCC (see General Part § 5 No. 2 and **Annex 2**):

Categories of data subjects whose personal data are processed

All persons whose personal data is contained in the content (texts, files) provided by the customer in AI Assist.

Categories of personal data that are processed

All data contained in the texts provided by the customer in AI Assist.

Sensitive data processed (if applicable) and restrictions or safeguards applied that take full account of the nature of the data and the risks involved, e.g. strict purpose limitation, access restrictions (including access only for employees who have undergone specific

training), records of access to the data, restrictions on onward transfers or additional security measures

Sensitive personal data is not specifically processed. If a text from the customer contains corresponding sensitive data, the customer will pseudonymize or anonymize this data before uploading the project to AI Assist, provided that the pseudonymization or anonymization of the data does not conflict with the fulfillment of the processing purpose.

Frequency of transmission (e.g. whether the data is transmitted once or continuously)

Continuously during the use of AI Assist by the customer.

Type of processing

Automated analysis of texts using artificial intelligence.

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

Automated analysis of texts using artificial intelligence.

Duration of the processing

The data provided by the customer in AI Assist will be processed for no longer than the duration of the contractual relationship. If processing is no longer necessary at an earlier point in time, the data will be deleted immediately.

In the case of processing by (sub)processors, the object, type and duration of the processing must also be specified.

When using AI Assist, data is stored on a cloud server and forwarded to a service provider for further processing using artificial intelligence methods. A regularly updated list of the service providers used can be found here: https://www.maxqda.com/subprocessors.

Processing is used to prepare the texts and for analysis. The data is processed for no longer than the duration of the contract.

1.2 The following information contains the relevant information for Attachment I Section A of the SCC:

Activities relevant to the data provided under these clauses:

Provision of AI Assist.

2. MAXQDA Transcription

2.1 The following information contains the relevant information for Attachment II of the DPA and Attachment I Section B of the SCC:

Categories of data subjects whose personal data are processed

All persons whose personal data are contained in the files provided by the customer for transcription via MAXQDA Transcription.

Categories of personal data that are processed

All data contained in the files provided by the customer for transcription via MAXQDA Transcription.

Sensitive data processed (if applicable) and restrictions or safeguards applied that take full account of the nature of the data and the risks involved, e.g. strict purpose limitation, access restrictions (including access only for employees who have undergone specific training), records of access to the data, restrictions on onward transfers or additional security measures.

Sensitive personal data will not be processed in a targeted manner. The customer shall take appropriate measures to prevent a file from containing sensitive data as far as possible, if this does not prevent the fulfillment of the purpose of processing.

Frequency of transmission (e.g. whether the data is transmitted once or continuously)

Continuously during the use of MAXQDA Transcription by the customer.

Type of processing

Automated transcription of an audio file using artificial intelligence.

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

Automated transcription of an audio file using artificial intelligence.

Duration of the processing

The data provided by the customer will be processed for no longer than the duration of the contractual relationship. If processing is no longer necessary at an earlier point in time, the data will be deleted immediately. In the case of an audio file uploaded to the "MAXQDA Account" website, the deletion takes place 7 days after upload and we delete the created transcript 7 days after download by the customer, if the customer does not initiate the deletion beforehand.

In the case of processing by (sub)processors, the object, type and duration of the processing must also be specified.

When using AI Assist, data is stored on a cloud server and passed on to a service provider for further processing using artificial intelligence methods. A regularly updated list of the service providers used can be found here: https://www.maxqda.com/subprocessors.

When using MAXQDA Transcription, data is stored on a cloud server and forwarded to a service provider for further processing using artificial intelligence methods. A regularly updated list of the service providers used can be found here: https://www.maxqda.com/subprocessors. The processing is used to prepare the files for transcription and for transcription by the service provider used. The data will be deleted immediately after processing is no longer necessary. In the case of an audio file uploaded to the "MAXQDA Account" website, the deletion takes place 7 days after upload and we delete the created transcript 7 days after download by the customer, if the customer does not initiate the deletion beforehand.

2.2 The following information contains the relevant information for Attachment I Section A of the SCC:

Activities relevant to the data provided under these clauses: Provision of AI Assist.

MAXQDA TeamCloud

This section only applies to customers who have concluded a contract with VERBI for the use of MAXQDA TeamCloud in addition to the use of the standard software "MAXQDA". The MAXQDA TeamCloud is currently only available to universities, research institutions and companies, but not to private customers.

§ 1 Subject matter of the contract

1. The subject matter of the contract is the use of MAXQDA TeamCloud for the storage of projects created with the standard software "MAXQDA".

2. The MAXQDA TeamCloud is hosted on servers of Amazon Web Services ("AWS"). The customer is aware that VERBI does not operate the MAXQDA TeamCloud on its own servers and that the provision is therefore subject to conditions that are not determined by VERBI but by AWS. The use of MAXQDA TeamCloud by the customer is therefore not only governed by these GTC/EULA, but is also subject to the AWS Service Terms, available at: https://aws.amazon.com/de/service-terms/. By agreeing to these GTC/EULA, the customer therefore also accepts the AWS Service Terms.

§ 2 Requirements for use

1. The requirement for the acquisition of a license for the use of MAXQDA TeamCloud is a subscription by the customer for the use of the standard software "MAXQDA" in accordance with the provisions of the GTC/EULA for the standard software "MAXQDA". In the case of other license types (e.g. purchase), license acquisition for MAXQDA TeamCloud is not possible. The pure use of MAXQDA TeamCloud is possible with any paid license (subscription and purchase).

2. The customer must create an online account to use MAXQDA TeamCloud.

§ 3 Scope

1. The permissible scope of use of MAXQDA TeamCloud by the customer shall be governed by these GTC/EULA and the AWS Service Terms (as amended from time to time, available online at: https://aws.amazon.com/de/service-terms/). In the event of a conflict or inconsistency between the AWS Service Terms and these GTC/EULA, the AWS Service Terms shall prevail to the extent of such conflict or inconsistency.

2. The customer has access to storage capacities of up to 25 GB in the MAXQDA TeamCloud standard configuration.

3. After purchasing a license for the use of MAXQDA TeamCloud, the customer designates a so-called TeamLead who can use and manage the MAXQDA TeamCloud. This TeamLead can invite

up to four other users (“Members”) to share the MAXQDA TeamCloud with him. The invitation is sent by email. Once the members have accepted the invitation, the TeamLead can add them to a project. Each member only has access to the projects to which they have been invited, regardless of the number of projects the TeamLead has in their MAXQDA TeamCloud Account.

§ 4 Restrictions on use

1. The customer is aware that sensitive data within the meaning of Art. 9 para. 1 of the General Data Protection Regulation (GDPR) are particularly worthy of protection. If a customer's project contains such sensitive data, the customer will pseudonymize or anonymize this data before uploading the project to the MAXQDA TeamCloud, provided that the pseudonymization or anonymization of the data does not conflict with the fulfillment of the processing purpose.

2. Furthermore, the customer is not permitted to store content in the MAXQDA TeamCloud that violates laws or the rights of third parties or infringes their rights or otherwise violates the provisions of these GTC/EULA or the AWS Terms.

3. In addition, the use of MAXQDA TeamCloud by the customer is subject to the restrictions arising from the AWS Terms. This also applies to possible restrictions on availability, for example in the case of maintenance.

§ 5 Term and termination

1. The use is limited in time to the duration of the underlying usage contract with VERBI.

2. Access to MAXQDA TeamCloud will be disabled for the customer after expiration of use. The customer is solely responsible for downloading all relevant data in time before expiry of the period of use.

§ 6 Data protection

§ Section 6 shall not apply insofar as the customer is a natural person and the processing of personal data is carried out during a purely personal or household activity.

1. The following information contains the relevant information for Attachment II of the DPA (see General Part § 5 No. 1 and **Annex 1**) and Attachment I Section B of the SCC (see General Part § 5 No. 2 and **Annex 2**):

Categories of data subjects whose personal data are processed

All persons whose personal data is contained in the projects stored by the customer in MAXQDA TeamCloud.

Categories of personal data processed

All data contained in the projects stored by the customer in MAXQDA TeamCloud.

Sensitive data transferred (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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Sensitive personal data is not specifically processed. If a project of the customer contains corresponding sensitive data, the customer will pseudonymize or anonymize this data before uploading the project to MAXQDA TeamCloud, provided that the pseudonymization or anonymization of the data does not prevent the fulfilment of the processing purpose.

Furthermore, the AWS security standards apply in the respective current version (Attachment 1 to the AWS Order Processing Agreement).

Frequency of transmission (e.g. whether the data is transferred on a one-off or continuous basis)

Continuously during the use of MAXQDA TeamCloud by the customer.

Nature of the processing

Hosting of the customer projects.

Purpose(s) of the data transfer and further processing

Storage of customer projects in the MAXQDA TeamCloud.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The duration of the agreement is based on the duration of the customer's subscription. Three months after the end of the contract, the customer's project data will be deleted from TeamCloud.

In the case of processing by (sub)processors, subject matter, nature and duration of the processing

The MAXQDA TeamCloud is stored on a cloud server from AWS. The processing serves the hosting of the MAXQDA Cloud. The duration of the processing is again based on the duration of the customer's subscription.

The Parties waive the obligation under clause 7.7 lit. (e), according to which the Processor is obliged to agree on a third-party beneficiary clause with the sub-processors.

2. The following information contains the relevant information for Attachment I Section A of the SCC:

Activities relevant to the data transferred under these clauses: Provision of MAXQDA TeamCloud.

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
STANDARD CONTRACTUAL CLAUSES

SECTION 1

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 Attachment 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 Attachment II.

(d) Attachments 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 Attachments 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 if 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]

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 Attachment 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 Attachment II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal

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

7.4. Security of processing

(a) The processor shall at least implement the technical and organizational measures specified in Attachment 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, unauthorized 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.

(a) 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 authorized 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.

(b) 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 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 consider relevant certifications held by the processor.

(c) 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.

(d) 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

(c) The processor has the controller's general authorization 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.

(a) 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.

(b) 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

(f) Any transfer of data to a third country or an international organization 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.

(g) 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 authorized 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 Attachment III the appropriate technical and organizational 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

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 Attachment 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.

ATTACHMENT 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.

ATTACHMENT II - DESCRIPTION OF THE PROCESSING

See relevant information in the respective data protection sections of these GTC.

ATTACHMENT III - TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL 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.

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
- Safety locks
- Locking system with code card
- Doorbell system with camera
- Careful selection of security staff

- Careful selection of the cleaning service

1.2 Access control

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

- Login with user name and password
- Use of anti-virus software
- Use of firewall software
- Use of VPN for remote access
- Creating user profiles
- Assigning and managing user authorizations
- Assigning passwords
- Guidelines for: "Secure password" and "Delete/destroy"

1.3 Access control

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

- Use of document shredders
- Physical deletation of data carriers
- Proper destruction of data carriers (DIN 32757)
- Logging of access to applications, specifically when entering, changing and deleting data
- Management of rights by system administrator
- Number of administrators reduced to the "bare minimum"

1.4 Separation 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 customer systems
- Providing the data records with purpose attributes/data fields
- Definition of database rights
- Control via authorization concept

1.5 Pseudonymization

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

- Internal instruction to anonymize / pseudonymize personal data as far as possible in the event of disclosure or after the statutory deletion period has expired.

2. Integrity (Art. 32 para. 1 lit. b GDPR)

2.1 Transfer control

• Measures to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transmission or during transport or storage on data carriers, and that it is possible to verify and establish to which bodies personal data are intended to be transmitted by data transmission equipment.

- Use of VPN
- Logging of accesses and retrievals
- Personal data that is passed on on behalf of customers is only passed on to the extent that this has been agreed with the customer or is necessary for the provision of the contractual service for the customer.
- Employees of VERBI GmbH who work in customer support are instructed with regard to the permissible use of data and the modalities of passing on data.
-

2.2 Entry control

Measures that ensure that it is possible to subsequently check and determine whether and by whom personal data has been entered, modified or removed from data processing systems.

- Technical logging of the entry, modification and deletion of data
- Overview of which programs can be used to enter, change or delete which data Forwarding
- Traceability of data entry, modification and deletion through individual user names (not user groups)
- Clear responsibilities for deletions and reminder system for deletion.

3. Availability and resilience (Art. 32 para. 1 lit. b GDPR)

Measures to ensure that personal data is protected against accidental destruction or loss.

- Fire and smoke detection system
- Server room temperature and humidity monitoring
- Air-conditioned server room
- Protective socket strips Server room
- Fire extinguisher Server room
- Uninterruptible power supply (UPS)
- Logging of accesses and retrievals
- Implementation of the backup & recovery concept
- Regular data recovery tests and logging of the results
- Storage of backup media in a secure location outside the server room
- No sanitary connections in or above the server room.

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

4.1 Data Protection measures

- Central documentation of all procedures and regulations on data protection with access for employees as required / authorized on the intranet
- Regular review of the effectiveness of the technical protection measures
- Engagement of an External Data Protection Officer
  - (kontakt@datenschutzrechte.de)
- A DST (Data Protection and Information Security Team) has been set up to planb, implement, evaluate and adjust measures in the area of data protection and data security
- The data protection impact assessment is carried out as required
- VERBI GmbH complies with the information obligations according to Art. 13 and 14 GDPR
- Formalized process for processing requests for information from data subjects is in place.

4.2 Incident-Response-Management

Support in responding to security breaches

- Use of firewall and regular updates
- Use of spam filters and regular updates
- Use of virus scanners and regular updates

- Support from IT crisis experts and data protection lawyers as part of cyber risk insurance
- Documentation of security incidents and data breaches, e.g. via ticket system
- All employees are instructed and trained to ensure that data protection incidents are recognized and reported to the DPO immediately.
- The training courses are held regularly to ensure that the content is continuously updated.

4.3 Data protection friendly default settings

Privacy by design / Privacy by default

- The principle of necessity and data minimization is taken into account.
- No more personal data is collected than is necessary for the respective purpose.

4.4 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 minimization is taken into account
- Conclusion of the necessary agreement on order processing or EU standard contractual clauses.
- A regularly updated list of third-party service providers and subprocessors can be found on our website.

Annex 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 Attachment 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 Attachment I.A. (hereinafter each "data importer"),

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

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, the use of these clauses when engaging another processor (subprocessor) not covered by Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC. (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), insofar as these clauses and the data protection obligations laid down in the contract or other legal instrument between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This is particularly the case if the controller and processor rely on the standard contractual clauses contained in Decision 2021/915.
.

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

(i) The Annex to these Clauses containing the Attachments referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(j) 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 Annex. 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.

(a) 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

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

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

(d) 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 Attachment 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 organizational 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

(e) The Parties shall implement appropriate technical and organizational 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, unauthorized 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 pseudonymization, including during transmission, where the purpose of processing can be fulfilled in that manner.

(f) 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.

(g) The data exporter shall ensure that persons authorized 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

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 authorized to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

Clause 12

Liability

(c) 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.

(d) 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.

(e) 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.

(f) 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.

(g) 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]

Klausel 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.

ANNEX

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 annexes for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one annex. However, where necessary to ensure sufficient clarity, separate annexes should be used.

ATTACHMENT 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: See relevant information in the respective sections on data protection of these GTCs

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: See relevant information in the respective sections on data protection of these GTCs

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

See relevant information in the respective data protection sections of these GTC.