

## Auftragsverarbeitungsvereinbarung

### Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28, 29 DSGVO

zwischen

**Example – to create the actual DPA visit [s2survey.net/DSGVO/](https://s2survey.net/DSGVO/)**

– Verantwortlicher, –  
– nachfolgend auch „**Auftraggeber**“ genannt –

und

vertreten durch die Geschäftsführer  
Dr. Dominik Leiner und Stefanie Leiner

– Auftragsverarbeiter, –  
– nachfolgend auch „**Auftragnehmer**“ genannt –

Beispiel GmbH  
Musterstraße 47  
12345 Musterstadt

SoSci Survey GmbH  
Erchanbertstr. 6  
81929 München

## Data Processing Agreement

### Agreement on the processing of personal data on behalf of a Controller pursuant to Art. 28 GDPR

between

– Controller, –  
– hereinafter also referred to as „**Ordering Party**“ –

and

represented by its Managing Directors  
Dr. Dominik Leiner and Stefanie Leiner

– Processor, –  
– hereinafter referred to as „**Contract Partner**“ –

Beide Vertragsparteien werden in nachstehender Vereinbarung auch einzeln als **Partei** und gemeinsam als **Parteien** bezeichnet.

Both contracting parties shall also individually be referred in the following terms to as „**Party**“ and collectively as the „**Parties**“.

## Präambel

Zwischen Auftraggeber und Auftragnehmer wurden eine oder mehrere Bestellungen getätigt und/oder separate Verträge abgeschlossen (nachfolgend als „Nutzungsvereinbarungen“ bezeichnet), welche die Nutzung der Dienstleistung des Auftragnehmers (nachfolgend als „Dienstleistung“ bezeichnet) als Software-as-a-Service (*SaaS*, auch *Cloud-Service*) regeln. Gegenstand der Dienstleistung sind Onlineumfrageprojekte auf dem Befragungsserver **s2survey.net** im Rahmen und auf Grundlage der hierfür vom Auftragnehmer zur Verfügung gestellten Software, wobei die Nutzungsvereinbarungen eine oder mehrere Umfragen (Befragungsprojekte) umfassen kann.

Die Nutzung der Dienstleistung erfordert die Registrierung eines Benutzerkontos durch den Auftraggeber auf Basis der Allgemeinen Geschäftsbedingungen (nachfolgend als „AGB“ bezeichnet) der SoSci Survey GmbH. Daraus resultiert ein Hauptvertrag zur Nutzung der Dienstleistung, welcher auf unbestimmte Zeit geschlossen wird/wurde und dessen vertraglichen Vereinbarungen sich aus den AGB ergeben. Allen

## Preamble

One or more purchase orders and/or specific contracts (hereinafter referred to as “purchase orders”) were agreed between the Controller and the Processor which determine the use of the Processor's service (hereinafter referred to as “service”) as Software-as-a-Service (*SaaS*, also *Cloud Service*). Subject of the service are online survey projects on the survey server **s2survey.net** within the framework and on basis of the software provided by the Processor, whereby the purchase orders may include one or more surveys (survey projects).

The use of the service requires the registration of a user account by the Controller on the basis of the General Terms and Conditions (hereinafter referred to as “Terms and Conditions”) of SoSci Survey GmbH. This results in a main contract governing the use of the service, which is/was concluded without contract term and whose contractual terms are de-

Nutzungsvereinbarungen liegen damit die AGB zugrunde.

Die Nutzungsvereinbarungen sehen für die Vertragserfüllung notwendig unter anderem eine Verarbeitung von personenbezogenen Daten durch den Auftragnehmer im Auftrag des Auftraggebers vor. Der Auftraggeber beauftragt den Auftragnehmer mit der Auftragsverarbeitung im Zusammenhang mit den Nutzungsvereinbarungen, wie vorab beschrieben. Die im Zusammenhang mit dem Hauptvertrag erhobenen personenbezogenen Daten sind nach Art, Zweck und Umfang in Anlage 1 zu dieser Vereinbarung näher beschrieben. Sollte die Verarbeitung von personenbezogenen Daten bei einem bestimmten Befragungsprojekt von der Beschreibung in Anhang 1 abweichen, verpflichten sich die Parteien, dies in einem Nachtrag niederzulegen.

Folgende Vereinbarung erläutert die datenschutzrechtlichen Verpflichtungen der Parteien, die sich aus der Beauftragung des Auftragnehmers und/oder durch die Nutzungsvereinbarungen ergeben. Diese Vereinbarung zur Auftragsverarbeitung (im Folgenden kurz: „AVV“) ergänzt den Hauptvertrag/Haupttätigkeit in datenschutzrechtlicher Hinsicht. Diese AVV findet Anwendung auf sämtliche Tätigkeiten, bei denen der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet. Begriffsdefinitionen richten sich nach den Datenschutzgesetzen, sofern deren Anwendbarkeit eröffnet ist.

Dies vorausgeschickt vereinbaren die Parteien wie folgt:

## 1. Anwendungsbereich, Auftragsgegenstand (Art. 28 Abs. 1 DSGVO)

- 1.1. Im Rahmen der Leistungserbringung nach dem, diesem AVV zugrundeliegenden Nutzungsvereinbarungen, ist es erforderlich, dass der Auftragnehmer Zugriff auf personenbezogene Daten des Auftraggebers, seiner insoweit eingebundenen Angestellten, Umfrageteilnehmer oder sonstiger betroffener Dritter erhält oder bei Inanspruchnahme der Dienstleistung durch Nutzung der Software des Auftragnehmers personenbezogene Daten erhält. Diese Daten werden nachfolgend einheitlich (personenbezogene) Daten genannt. Im Zuge der Durchführung der Haupttätigkeit/Hauptvertrag wird der Auftragnehmer vom Auftraggeber mit der Verarbeitung der vertragsgegenständlichen Daten im Rahmen der angebotenen Softwarelösung beauftragt. Diese AVV konkretisiert die datenschutzrechtlichen Rechte und Pflichten

rived from the Terms and Conditions. All purchase orders are thus based on the Terms and Conditions.

The purchase orders require, among other provisions, the processing of personal data by the Processor on behalf of the Controller. The Controller shall instruct the Processor with the data processing related to the purchase orders described above. The personal data collected in the course of the purchase orders is described in more detail in Annex 1 to this Agreement in terms of type, purpose and scope. Should the processing of personal data in a specific survey project deviate from what is described in Annex 1, the Parties commit themselves to entering it in an addendum.

The following agreement explains the data protection obligations of the parties arising from the assignment of the Processor by the purchase orders. This data processing agreement (hereinafter referred to as "DPA") complements and/or supplements the purchase orders in terms of data protection law. This DPA shall apply to all services in which the Processor processes personal data on behalf of the Controller. Definitions of terms are based on the data protection laws, insofar applicable.

In consideration of the foregoing, the parties agree as follows:

## Contract Scope, Subject matter (section 28 para. 1 GDPR)

Within the framework of the provision of services according to the purchase orders on which this DPA is based, it is required that the Processor obtains access to personal data of the Controller, its employees, survey participants or other affected third parties or, if the main service is used, obtains personal data by using the Processor's software. This data is hereinafter uniformly referred to as contractual data. In the course of performing the service, the Processor shall be commissioned by the Controller to process the contractual data within the framework of the software solution offered. This DPA specifies the data protection rights and obligations of the contracting parties in the performance of the purchase orders.

ten der Vertragsparteien bei der Durchführung der Nutzungsvereinbarungen.

- 1.2. Gegenstand der Tätigkeit des Auftragnehmers ist nicht die originäre Verarbeitung von personenbezogenen Daten. Im Zuge der Leistungserbringung des Auftragnehmers im Rahmen der Nutzungsvereinbarungen kann ein Zugriff auf personenbezogene Daten jedoch nicht ausgeschlossen werden.

- 1.3. Als "Datenschutzgesetze" im Sinne dieser Vereinbarung gelten die Datenschutzgrundverordnung (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates, nachfolgend „DSGVO“) und, sofern auf den Auftraggeber anwendbar, die Neufassung des Bundesdatenschutzgesetzes („BDSG“) von 2018, die Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates (nachfolgend „EDPR“) und das Landesdatenschutzgesetz (LDSG).

Wenn die Bestimmungen der vorgenannten Gesetze und Verordnungen denselben Grundsätzen folgen, sollten sie einheitlich ausgelegt werden.

- 1.4. Alle Begrifflichkeiten dieses AVV werden im Sinn und im Verständnis nach den Datenschutzgesetzen verwendet, wobei insbesondere

- **„personenbezogene Daten“** gemäß Art 4 Ziffer 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen bedeutet. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.
- **„Verarbeitung“** bezeichnet gemäß Art 4 Ziffer 2 DSGVO jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Subject of the processor's services is not primary processing of personal data. However, access to personal data cannot be precluded in the course of the processor's service performance within the scope of the purchase orders.

For the purposes of the present Agreement, "Data Protection Laws" means the Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council, hereinafter referred to as "GDPR"), and if applicable to the Processor, the new version of the German Federal Data Protection Act (Bundesdatenschutzgesetz 2018, "BDSG") and the European Data Protection Regulation (Regulation (EU) 2018/1725, hereinafter referred to as "EDPR") and the State Data Protection Act (Landesdatenschutzgesetz).

Whenever the provisions of the above laws and regulations follow the same principles, they should be interpreted homogeneously.

All terms of this DPA are used in accordance and understanding of the data protection laws, whereby in particular

- **"Personal data"** means according to section 4 clause 1 GDPR any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- **"Processing"** means pursuant to section 4 clause 2 GDPR any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- 1.5. Die Vertragsparteien ergänzen und konkretisieren mit der gegenständlichen AVV die gegenseitigen Pflichten im generellen Umgang mit den vom Auftraggeber zur Verfügung gestellten Daten oder den für ihn erhobenen Daten. Im Falle eines Widerspruchs zwischen den Bestimmungen dieser Vereinbarung und denjenigen der Nutzungsvereinbarungen gehen die Bestimmungen dieser AVV vor.

With this DPA the contracting parties supplement and specify the mutual duties in the overall handling of the data provided by the processor or the data collected for him. In the event of a contradiction between the provisions of this DPA and those of the underlying purchase orders, the provisions of this DPA shall prevail.

## 2. Bestimmung des Auftragsgegenstandes, Laufzeit

## Specification of the subject matter, duration

- 2.1. Umfang, Art und Zweck der Aufgaben des Auftragnehmers zur Verarbeitung von Daten in Bezug auf den Auftragsgegenstand ergeben sich aus den Nutzungsvereinbarungen. Die Verarbeitung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der einschlägigen datenschutzrechtlichen Vorschriften, insbesondere die Vorschriften zu Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen, erfüllt sind.
- 2.2. Die vertragsgegenständlichen Daten werden vom Auftragnehmer ausschließlich im Auftrag und nach Weisungen des Auftraggebers im Sinne von Art. 28, 29 DSGVO (Auftragsverarbeitung) verarbeitet. Verantwortlicher im Sinn der Datenschutzgesetze bleibt der Auftraggeber und dieser trägt somit die Verantwortung für die Rechtmäßigkeit der auftragsgemäßen Verarbeitung der vertragsgegenständlichen Daten. Der Auftragnehmer wird diese Daten daher nur auf Weisung des Auftraggebers verarbeiten, wie nachstehend in Ziffer 5 weiter festgelegt. Die Verantwortlichkeit des Auftraggebers bezieht sich insbesondere darauf, dass die vertrags- und weisungsgemäße Datenverarbeitung rechtmäßig ist, die Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden und deren Einhaltung nachgewiesen werden kann.
- 2.3. Die Art der betroffenen vertragsgegenständlichen Daten und die Kategorien der durch die Verarbeitung betroffenen Personen sind in **Anlage 1** abschließend normiert.
- 2.4. Die Laufzeit dieser Vereinbarung ist befristet bis zum **31.10.2022**. Der Vertrag beginnt mit der Unterzeich-

The scope, nature and purpose of the Processor's duties by processing data regarding the subject matter shall be governed by the purchase orders. The processing of data solely takes place in the territory of the Federal Republic of Germany, in a member state of the European Union or in another contracting state of the Agreement on the European Economic Area. Any transfer to a third country requires the prior written consent of the Controller and may only take place if the special requirements of the relevant data protection laws, in particular the regulations on the transfer of personal data to third countries or to international organizations are fulfilled.

The Processor shall process the contract data solely on behalf of and in accordance with the instructions of the Controller within the meaning of Art. 28, 29 GDPR (data processing). The Controller remains legally responsible in terms of Data Protection Laws and thus bears the responsibility for the legality of the order-compliant processing of the contractual data. The Processor shall therefore only process the data on basis of instructions of the Controller, as further specified in Section 5 below. The responsibility of the Controller refers in particular to the fact that the data processing is in accordance with the contract, as directed and is lawful, also that the principles for processing of personal data are observed and that their compliance can be proven.

The nature of the relevant contractual data and the categories of persons affected by the processing are conclusively defined in **Annex 1**.

The term of this DPA shall expire on **31.10.2022**. The contract term begins with the signing of this DPA,

**Example – to create the actual DPA visit [s2survey.net/DSGVO/](https://s2survey.net/DSGVO/)**

nung der vorliegenden Vereinbarung, nicht jedoch vor Wirksamkeit der zugrunde liegenden Hauptleistungsververeinbarung. Ziffer 14.1 bleibt hiervon unberührt.

- 2.5. Die Parteien sind sich bewusst, dass die Auftragsverarbeitung nicht ohne wirksame AVV erfolgen darf, sodass die Auftragsverarbeitung im Falle der Beendigung der gegenständlichen AVV bis zum Abschluss einer neuen AVV über die Verarbeitung personenbezogener Daten im Auftrag trotz bestehenden Nutzungsververeinbarungen nicht erfolgen darf. Spiegelbildlich ist Gegenstand dieser AVV nicht die originäre Nutzung oder Verarbeitung von personenbezogenen Daten durch den Auftragnehmer, dennoch kann im Zuge der Hauptleistungserbringung ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden. Erfolgt damit keine zu erbringende Hauptleistung während der Laufzeit dieser AVV, berechtigt diese AVV allein den Auftragnehmer ebenfalls nicht zur Verarbeitung personenbezogener Daten im Auftrag. Hierfür bedarf es einer zugrundeliegenden Hauptleistung.

### 3. Technische und organisatorische Maßnahmen (TOM)

- 3.1. Der Auftragnehmer gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den Anforderungen des Datenschutzes gerecht wird. Er trifft dabei technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten vor Missbrauch und Verlust, die den Anforderungen der DSGVO entsprechen. Soweit es den Parteien erforderlich erscheint, kann dem Auftraggeber ein Verzeichnis der technisch-organisatorischen Maßnahmen mit Vertragsschluss übergeben werden.
- 3.2. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Der Auftragnehmer ist verpflichtet, die technischen und organisatorischen Maßnahmen dem Stand der Technik anzupassen. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Die durch den Auftragnehmer bei Beginn der Verarbeitung umgesetzten technischen und organisatorischen Maßnahmen sind in Anlage 3 aufgeführt. Bei geringfügigen Änderungen an den technischen und organisatorischen Maßnahmen (z.B. Ersatz der Schließanlage durch eine neue, jedoch gleichwertige) ist die Änderung lediglich zu dokumentieren. Bei wesentlichen Änderungen (z.B. grundlegende Änderung von Verschlüsselungssystemen)

but not prior to the effective date of the underlying main contract. Section 14.1 remains unaffected by this provision.

The Parties are aware that data processing may not take place without an effective DPA despite existing purchase orders, so that data processing may not proceed in the event of termination of the present DPA until the signing of a new DPA on processing of personal data. The primary use or processing of personal data by the Processor is not the subject of these DPA, nevertheless access to personal data cannot be precluded in the course of providing the main service. If there is no main service to be provided during the term of this DPA, this DPA itself shall not entitle the Processor to process personal data. This requires an underlying main performance.

### Technical and organizational measures (TOM)

Within its area of responsibility, the Processor shall arrange his internal organization under his responsibility in such a way that it meets the requirements of data protection. He shall take technical and organizational measures to reasonably secure the data against abuse and loss in accordance with the requirements of the GDPR. If deemed necessary by the parties, a list of technical and organizational measures can be handed over to the Controller upon signature of the contract.

The technical and organizational measures are subject to technical progress and further development. The Processor is obliged to adapt the technical and organizational measures to the state of the art. In this respect, the Processor shall be permitted to implement alternative adequate measures. In doing so, the security level of the specified measures may not be undercut. The technical and organizational measures implemented by the Processor at the start of processing are listed in Annex 3. In the case of minor changes to the technical and organizational measures (e.g. replacement of the locking system with a new but equivalent one), the change need only be documented. In the case of major changes (e.g. fundamental changes to encryption systems), the Controller's written consent must be obtained in advance. At the request of the Controller, the Processor

men) ist vorab die schriftliche Zustimmung des Auftraggebers einzuholen. Der Auftragnehmer hat auf Anforderung des Auftraggebers an der Erstellung der Verzeichnisse des Auftraggebers, die die Auftragsverarbeitung nach dieser Vereinbarung betreffen, mitzuwirken, insbesondere die hierfür erforderlichen Angaben des Auftraggebers zur Verfügung zu stellen.

- 3.3. Solange das angemessene und vereinbarte Schutzniveau nicht unterschritten wird und dem Stand der Technik entspricht, hat der Auftraggeber seine Zustimmung zu erteilen, außer wichtige Gründe stehen der Einführung entgegen. Geringfügige Änderungen werden nur als Ergänzung zu den technisch-organisatorischen Maßnahmen vom Auftragnehmer dokumentiert. Alle Vorabversionen der technisch-organisatorischen Maßnahmen werden vom Auftragnehmer zum Nachweis geringfügiger Abweichungen dokumentiert
- 3.4. Bei der Verarbeitung personenbezogener Daten ist der Auftragnehmer verpflichtet, die datenschutzrechtlichen Grundsätze einzuhalten sowie die Sicherheit herzustellen, die zum Schutz personenbezogener Daten erforderlich ist. Insgesamt handelt es sich bei allen zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme (Art. 32 Abs. 1 lit. b DSGVO). Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen.

#### 4. Qualitätsmanagement, Verpflichtungen des Auftragnehmers

Ergänzend zur Einhaltung der Regelungen dieser Vereinbarung hat der Auftragnehmer weitere datenschutzrechtliche Pflichten. Er gewährleistet insbesondere die Einhaltung folgender Vorgaben:

shall cooperate in the preparation of the Controller's processing directories relating to the commissioned processing under this Agreement, and in particular shall provide the Controller with the information required for this purpose.

As long as the level of protection does not fall below the appropriate and agreed level and as long as the state of the art complies, the Controller must give his consent, unless there are important reasons for not being introduced. Minor changes shall only be documented by the Processor as a supplement to the technical and organizational measures. All preliminary versions of the technical-organizational measures shall be documented by the Processor to prove minor deviations.

When processing personal data, the Processor is obliged to comply with the principles of Data Protection Laws and to provide the security required for the protection of personal data. Overall, all measures to be taken shall be data security measures and shall ensure a level of protection appropriate to the risk, in terms of confidentiality, integrity, availability and resilience of the systems (section 32, para. 1 lit. b GDPR). It shall be taken into account the state of the art, the implementation costs and the nature, scope and purpose of processing as well as the different likelihood and severity of the risk to the rights and freedoms of natural persons.

#### Quality Management, Processor Obligations

In addition to compliance with the provisions of this agreement, the Processor shall have further data protection obligations. In particular, he shall ensure compliance with the following requirements:



- 4.1. Soweit gesetzlich vorgeschrieben, die Bestellung eines Datenschutzbeauftragten (in schriftlicher Form), der seine Tätigkeit nach Maßgabe der datenschutzrechtlichen Vorschriften ausüben kann. Eine Neubesetzung des Datenschutzbeauftragten und/oder dessen Kontaktdaten während der Dauer dieser Vereinbarung ist dem Auftraggeber unverzüglich schriftlich mitzuteilen. Sofern keine Bestellung erfolgt, benennt der Auftragnehmer einen Ansprechpartner oder eine Ansprechpartnerin für den Datenschutz.
- 4.2. Die Wahrung der Vertraulichkeit, wobei der Auftragnehmer bei der Ausführung der Arbeiten ausschließlich Beschäftigte einsetzt, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie durch das Recht der Europäischen Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet sind. In einem solchen Fall teilt der Auftragnehmer dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Die Vertraulichkeitsverpflichtung des Auftragnehmers ist diesem Vertrag als Anlage 2 beigelegt.
- 4.3. Die Umsetzung und Berücksichtigung aller für diese Vereinbarung notwendigen technischen und organisatorischen Maßnahmen entsprechend dem Stand der Technik.
- 4.4. Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diese Vereinbarung beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
- 4.5. Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftragnehmer im Hinblick auf die Vertragsausführung bzw.-erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des AVV.
- 4.6. Auf Anfrage Auskunft über die getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber. Hierfür kann der Auftragnehmer auch geeignete und aktuelle Testate, Berich-

If required by law, he ensures the appointment of a data protection officer (in writing) who can perform his duties in accordance with data protection regulations. The appointment of another data protection officer during the term of this agreement and/or his contact data must be reported to the Controller immediately in writing. If no appointment is made, the Processor shall name a contact person who is in duty to ensure data protection.

Maintaining confidentiality, whereby the Processor shall only use employees in the performance of the work who have been obligated to maintain confidentiality and have previously been familiarized with the data protection provisions relevant to them. The Processor and any person subordinate to the Processor who has access to personal data shall process such data exclusively in accordance with the Controller's instructions, including the powers granted in this Agreement, unless they are required to process such data by European Union or Member State law. In such a case, the Processor shall notify the Controller of such legal requirements prior to the processing, unless the relevant law prohibits such notification due to an important public interest. The Processor's confidentiality undertaking is attached to this Contract as Annex 2.

The implementation and consideration of all technical and organizational measures necessary for this agreement with accordance to the state of the art.

The immediate information of the Controller about control actions and measures of the supervisory authority, insofar as the measures refer to this agreement. This shall also apply if a responsible authority investigates against the Processor within the framework of an administrative offence or criminal proceeding in the course of processing of personal data at the Processors premises.

Execution of the internal control by means of regular audits, including inspections by the Processor with regard to the execution or fulfilment of the contract, in particular compliance with and, if necessary, the required adaptation of regulations and measures for the implementation of the DPA.

Upon request, provide access and information to the Controller about technical and organizational measures. For this purpose, the Processor may also submit appropriate, current and up-to-date certificates,

te oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT- Sicherheitsabteilung, Datenschutzauditor, Qualitätsauditor) oder eine geeignete und aktuelle Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) vorlegen.

reports or report extracts from independent bodies (e.g. auditors, data protection officers, IT security departments, data protection auditors, quality auditors) or a suitable, current and up to date certificates if an IT security or data protection audit (e.g. according to BSI-Basic Protection "BSI-Grundschutz").

## 5. Weisungsbefugnis des Auftraggebers

- 5.1. Die Daten sind ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers gemäß Art. 28, 29 DSGVO bzw. Art. 29 EDPR zu verarbeiten. Weisungen des Auftraggebers sind durch beide Parteien zu dokumentieren. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, welches er durch Einzelweisungen näher bestimmen kann. Veränderungen des Verarbeitungsgegenstands und Verfahrensanpassungen sind zwischen den Parteien gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen bedürfen der vorherigen schriftlichen Genehmigung seitens des Auftraggebers.
- 5.2. Weisungen des Auftraggebers erfolgen ausschließlich in Textform (schriftlich oder per E-Mail). Dem Auftragnehmer ist es untersagt, die Daten für andere Zwecke zu nutzen und er ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate dürfen ohne Wissen des Auftraggebers nicht erstellt werden, ausgenommen davon sind Sicherheitskopien, jedoch nur, sofern und soweit diese zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, und Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
- 5.3. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung dieser Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.
- 5.4. Bei einer wesentlichen Änderung des Auftrags durch eine Weisung hinsichtlich der Datenverarbeitung steht dem Auftragnehmer ein Widerspruchsrecht zu. Besteht der Auftraggeber trotz des Widerspruchs des Auftragnehmers auf der Änderung, etwa die Umprogrammierung der Verarbeitungssoftware für Onlineumfragen, so ist diese Änderung als wichtiger Grund für den Auftragnehmer anzusehen und er-

## Authority of the Controller (to issue instructions)

The data shall be processed exclusively within the framework of this DPA and in accordance with the instructions of the Controller pursuant to Art. 28, 29 GDPR, or Art. 29 EDPR, respectively. Instructions from the Controller must be documented by both parties. Within the scope of the descriptions and provisions made in this agreement, the Controller reserves the comprehensive right to issue instructions over kind, scope and procedure of data processing, which he can specify in more detail by means of individual instructions. Changes to the processing matter and procedural adaptations shall be agreed and documented jointly between the parties. Any information to third parties or those affected requires the prior written consent of the Controller.

Instructions of the Controller shall solely be given in text form (in writing or by e-mail). The Processor is prohibited from using the data for other purposes and is in particular not entitled to pass them on to third parties. Copies and duplicates must not be made without the Controller's knowledge, with the exception of back-up copies to the extent required to ensure correct data processing, and data required for compliance with legal retention requirements.

The Processor must inform the Controller without delay if he is of the opinion that an instruction violates Data Protection Laws. The Processor is entitled to suspend the execution of any such instruction until the instruction has been confirmed and approved or changed by the responsible person at the Controller's organization.

In the event of a substantial change to the contract due to instructions regarding data processing, the Processor shall have the right to object. If, despite the Processor's objection, the Controller insists on the change, such as the reprogramming of the processing software for online surveys, this change and instruction shall be understood as substantial reason for the Processor which allows the termination of



laubt eine fristlose Kündigung des von der Weisung betroffenen AVV sowie der von der AVV betroffenen Bestandteile der entsprechenden Nutzungsvereinbarungen.

- 5.5. Ansprechpartner beim Auftraggeber für die Durchführung dieses Vertrages ist/sind

**Alberta Beispiel**

Telefon: +49 (89) 1234- 5678

E-Mail: a.beispiel@example.com

**Clemens Druckmann**

Telefon: +49 (89) 1234- 9876

E-Mail: c.druckmann@example.com

Anschrift wie Auftraggeber

Der Ansprechpartner ist zugleich die Person, die gegenüber dem Auftragnehmer berechtigt ist, datenschutzrechtliche Weisungen nach diesem Vertrag zu erteilen.

- 5.6. Ansprechpartner beim Auftragnehmer für die Durchführung dieses Vertrages ist:

**Dr. Dominik Leiner**

Telefon: +49 (163) 7952646

E-Mail: privacy@soscisurvey.de

Anschrift wie Auftragnehmer

Der Ansprechpartner ist zugleich die Person, die gegenüber dem Auftraggeber berechtigt ist, datenschutzrechtliche Weisungen nach diesem Vertrag zu empfangen.

- 5.7. Die Parteien können ihre Ansprechpartner jederzeit ändern. Es können mehrere Ansprechpartner benannt werden, die jeweils einzeln weisungs- bzw. empfangsberechtigt sind. Ist der Ansprechpartner einer Partei mehr als nur vorübergehend nicht erreichbar, hat die Partei den Ansprechpartner jedenfalls für die Dauer der Nichterreichbarkeit zu ändern. Die Änderung eines Ansprechpartners hat in dokumentierter Form zu erfolgen.

## 6. Überprüfungsrechte des Auftragsgebers, Kontrollrechte und Auftraggeberpflicht

Der Auftraggeber hat den Auftragnehmer unter dem Aspekt ausgewählt, dass dieser geeignete technische und organisatorische Maßnahmen (TOM) aufgesetzt hat, dass die Verarbeitung im Einklang mit den Anforderungen der Datenschutzgesetze erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet. Der Auftraggeber ist befugt, im Vorfeld der Datenverarbeitung und sodann regelmäßig die Einhaltung der datenschutzrechtlichen Pflichten des Auftragnehmers zu kontrollieren oder durch im Ein-

the DPA without notice as well as the relevant provisions of the corresponding purchase orders affected by the DPA.

Contact person at the Controller for the execution of this contract is/are:

**Alberta Beispiel**

Phone: +49 (89) 1234- 5678

E-mail: a.beispiel@example.com

**Clemens Druckmann**

Phone: +49 (89) 1234- 9876

E-mail: c.druckmann@example.com

Same address like Controller

The contact person is at the same time the person who is entitled vis-à-vis the Processor to issue data protection-related instructions in accordance with this contract.

Contact person at the Processor for the execution of this contract is:

**Dr. Dominik Leiner**

Phone: +49 (163) 7952646

E-mail: privacy@soscisurvey.de

Address like Processor

The contact person is at the same time the person who is entitled vis-à-vis the Controller to receive data protection instructions in accordance with this contract.

The parties may change their contact persons at any time. Several contact persons can be named, each of whom is individually authorized to issue instructions or receive instructions. If the contact person of a party is more than temporarily unavailable, the party shall change the contact person in any case for the duration of the unavailability. The change of a contact person must be documented.

## Controller's Inspection Rights, Control Rights, and Controller Obligations

The Controller has selected the Processor under the aspect that he has established suitable technical and organizational measures (TOM), that the processing is carried out in accordance with the requirements of the Data Protection Laws and that it guarantees the protection of the rights of the persons concerned. The Controller is entitled to preliminarily verify and henceforth on a regular basis the compliance of the Processor's service with his data protection duties and or to have them checked by auditors

Example – to create the actual DPA visit [s2survey.net/DSGVO/](https://s2survey.net/DSGVO/)

zufall zu benennende Prüfer kontrollieren zu lassen. Die Kontrollen beziehen sich insbesondere auf die vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen, die er gemäß den Bestimmungen dieser AVV treffen muss, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Der Auftraggeber oder ein anderer vom Auftraggeber beauftragter Prüfer ist zudem befugt, durch Stichprobenkontrollen und sonstige, auch Vor-Ort-Kontrollen, die gegebenenfalls angemessen anzumelden sind, die Einhaltung dieser AVV durch den Auftragnehmer in dessen Geschäftsbetrieb zu überprüfen. Der Auftragnehmer ist verpflichtet, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen.

Wenn in einer Prüfung eine oder mehrere Abweichungen von den dokumentierten Anweisungen des Auftraggebers festgestellt werden, hat der Auftragnehmer unverzüglich alle erforderlichen Korrekturmaßnahmen zu ergreifen, um die ordnungsgemäße Verarbeitung zu gewährleisten.

## 7. Betroffenenrechte

Der Auftragnehmer ist verpflichtet, Anträgen auf Ausübung von Datenschutzrechten gemäß Kapitel 3 DSGVO (z.B. Berichtigung oder Löschung der vertragsgegenständlichen Daten), sofern anwendbar, nur nach Weisung des Auftraggebers zu entsprechen. Soweit sich ein Betroffener zur Wahrnehmung seiner Betroffenenrechte (z.B. auf Auskunft, Berichtigung oder Löschung) unmittelbar an den Auftragnehmer wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

## 8. Unterstützungs- und Mitteilungspflichten, Datenschutz-Folgenabschätzung

Der Auftragnehmer hat den Auftraggeber bei der Erfüllung der datenschutzrechtlichen Pflichten zur Sicherheit personenbezogener Daten zu unterstützen, bei der Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel 3 der DSGVO genannten Rechte der betroffenen Person, ebenso bei Datenschutz-Folgeabschätzungen und vorherigen Konsultationen. Zu seinen Pflichten im Zusammenhang gehören insbesondere:

- 8.1. die Wahrung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, welche die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Si-

to be appointed in individual cases. The inspections relate in particular to the technical and organizational measures taken by the Processor, which he must establish in accordance with the provisions of these DPA in order to ensure a level of protection appropriate to the given risk. The Controller, or another auditor mandated by the Controller, shall be entitled to check the Processor's compliance with the DPA during his business operations by means of random inspections and other checks, including on-site inspections, for which appropriate notification may be required. Upon request, the Processor shall be obliged to provide the Controller with the necessary information and to make the relevant records available.

If, as a result of an audit, one or more non-conformities with the Controller's documented instructions are identified, the Processor shall promptly take all necessary corrective measures to achieve the required compliance.

## Rights of Data Subjects

The Processor is obliged to comply with requests to exercise data protection rights in accordance with Chapter 3 GDPR (e.g. rectification or deletion of the contractual data), if applicable, only under the Controller's instructions. Insofar as an affected person (data subject) should directly contact the Processor in order to claim his rights (e.g. for access and information, rectification or erasure), the Processor shall forward this request to the Controller without delay.

## Support and Information duties, Data Protection Impact Assessment (DPIA)

The Contractor shall support the Client in the fulfillment of data protection obligations regarding the security of personal data, in the obligation to respond to requests to exercise the rights of the data subject referred to in Chapter 3 of the GDPR, as well as in data protection impact assessments and prior consultations. His duties in this context include in particular:

the maintenance of an adequate level of protection through technical and organizational measures which consider the circumstances and purposes of the processing as well as the likelihood and severity of a possible infringement by security breaches and

- cherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen,
- 8.2. die Verpflichtung, alle Verletzungen der Datensicherheit, die sich auf die personenbezogenen Daten auswirken („Verletzung personenbezogener Daten“), dem Auftraggeber unverzüglich, spätestens jedoch innerhalb von 36 Stunden zu melden, nachdem er von den Sicherheitsverletzungen Kenntnis erlangt hat. Der Auftragnehmer muss dem Auftraggeber mindestens die folgenden Informationen zur Verfügung stellen:
- a) Art der Datenschutzverletzung und, soweit möglich, der Kategorien und die ungefähre Anzahl der betroffenen Personen sowie der Kategorien und der ungefähren Anzahl der betroffenen Datensätze;
  - b) wahrscheinliche Folgen der Verletzung;
  - c) Maßnahmen, die ergriffen oder vorgesehen wurden, um die Verletzung zu beheben und, sofern zutreffend, Maßnahmen zur Milderung ihrer möglichen Auswirkungen.
- 8.3. die Verpflichtung, den Auftraggeber bei der Untersuchung, Milderung und Behebung derartiger Verletzungen personenbezogener Daten sowie bei der Erfüllung von datenschutzrechtlichen Meldepflichten gegenüber der Aufsichtsbehörde zu unterstützen.
- 8.4. die Verpflichtung, den Auftraggeber im Rahmen seiner Pflicht zur Beantwortung von Anträgen der betroffenen Personen, welche die in Kapitel 3 DSGVO genannten Rechte wahrnehmen, zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen,
- 8.5. die Unterstützung des Auftraggebers bei dessen Datenschutz-Folgenabschätzung, sowie
- 8.6. die Unterstützung des Auftraggebers im Rahmen von Konsultationen der Aufsichtsbehörde. Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat der Auftragnehmer ihn nach besten Kräften zu unterstützen. Der Auftraggeber wird dem Auftragnehmer hierfür unverzüglich nach Erhalt eines Auskunftsersuchens, jedoch spätestens 14 Tage vor Ablauf der Monatsfrist gemäß Art. 12 Abs.3 DSGVO, mitteilen, wozu er konkret Auskünfte erteilen soll.
- 8.7. die Duldung von Kontrollen nach Ziffer 6 dieses AVV.
- enable an immediate detection of the relevant infringement events,
- the obligation to report any security breaches impacting the personal data (“personal data breach”) to the Controller without undue delay and at the latest within 36 hours after becoming aware of the security breaches. The Processor shall provide the Controller with at least the following information:
- a) nature of the personal data breach including where possible, the categories and approximate number of persons affected and the categories and approximate number of personal data records concerned;
  - b) likely consequences of the breach;
  - c) measures taken or proposed to be taken to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.
- the obligation to support the Client in investigating, mitigating and remedying such personal data breaches and in complying with data protection reporting obligations to the supervisory authority.
- the obligation to assist the Controller within the scope of its duty to respond to requests from data subjects exercising the rights referred to in Chapter 3 of the GDPR and, in this context, to provide the Controller with all relevant information without undue delay,
- the support of the Controller in his data protection impact assessment (DPIA), as well as
- assisting the Controller during consultations through the supervisory authority. Insofar as the Controller is subject to inspections and monitoring by the supervisory authority, an administrative offence or criminal proceeding, a liability claim of a data subject or a third party or any other claim in connection with processing activities in the Processor’s business, the Processor shall support the Controller to the best of his ability. The Controller shall inform the Processor immediately upon receipt of a request for access and information, but no later than 14 days before expiry of the monthly period pursuant to Art. 12 para. 3 GDPR, about the specific access and information he shall provide.
- toleration of inspections according to Section 6 of this DPA.

## **9. Verpflichtung zur Datenlöschung, Rückgabe von Datenträgern**

- 9.1. Während eines laufenden Befragungsprojekts im Rahmen der Nutzungsvereinbarungen wird der Auftragnehmer die vertragsgegenständlichen Daten nur auf Anweisung des Auftraggebers berichtigen, löschen, vernichten oder deren Verarbeitung einschränken.
- 9.2. Der Auftraggeber legt die Maßnahmen zur Rückgabe der überlassenen Daten und/oder deren Löschung der gespeicherten Daten nach Beendigung einer Onlineumfrage im Rahmen der Beauftragung durch den Hauptvertrag vertraglich oder durch Weisung fest. Der Auftragnehmer berichtigt oder löscht demgemäß die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies von seinem Weisungsrahmen umfasst ist.
- 9.3. Dem Auftraggeber steht im System bei Zugängen, die ihm durch den Auftragnehmer eingerichtet worden sind, selbst die vollständige Löschmöglichkeit der Daten einer Onlineumfrage zur Verfügung, wofür ihm deswegen die eigene Datenlöschungspflicht obliegt. Das System stellt dem Auftraggeber bis zur Löschung die Möglichkeit zum Herunterladen der Daten und damit zur Rückgabe der Daten zur Verfügung.
- 9.4. Mit Ende der jeweiligen Nutzungsvereinbarung oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Auftragsverarbeitung – hat der Auftragnehmer dem Auftraggeber auf Weisung alle Unterlagen in seinem Besitz, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, zu übergeben oder nach vorheriger schriftlicher Zustimmung des Auftraggebers datenschutzgerecht zu vernichten, sofern nicht nach dem Recht der Europäischen Union oder der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Die Löschung bzw. Vernichtung von Datenträgern und Material mit personenbezogenen Daten hat der Auftragnehmer dem Auftraggeber mit Datumsangabe schriftlich zu bestätigen. Der Auftragnehmer ist dabei weiter verpflichtet sicherzustellen, dass Datenträger und Material mit personenbezogenen Daten entweder durch eigene Datenvernichter (Reißwolf) oder von qualifizierten Entsorgungsunternehmen vernichtet werden, welche die Vernichtung schriftlich garantieren und bestätigen. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

## **Obligation to Data Erasure, Return of Data Carriers**

During an ongoing survey project within the contract term of the purchase orders, the Processor shall correct, delete, destroy or restrict the processing of the contractual data only on the instructions of the Controller.

The Controller shall, contractually or by instruction, determine the measures for returning the data provided and/or for the erasure of the stored data after termination of an online survey project under the terms of the main contract. The Processor corrects or deletes the contractual data accordingly, if the Controller instructs him accordingly and this is covered by his instruction rights.

In the case of an access which has been set up by the Processor for the Controller, the Controller himself has the entire erasure options for all data in the online survey available in the system and for which the Controller has his own data erasure duties. The system provides the client with the option of downloading the data and thus returning it until it is deleted.

At the end of the respective usage agreement or earlier upon request by the Controller – at the latest upon termination of the commissioned processing – the Processor shall hand over to the Controller upon instruction all documents in its possession, created processing and usage results as well as data files related to the commissioned relationship or destroy them in accordance with data protection law after prior written consent of the Controller, unless there is an obligation to store the personal data under the law of the European Union or the Member States. The Processor shall confirm the deletion or destruction of data carriers and material containing personal data to the Controller in writing, stating the date. The Processor is further obliged to ensure that data carriers and material with personal data are destroyed either by its own data shredders or by qualified disposal companies, which guarantee and confirm the destruction in writing. The same applies to test and scrap material. The protocol of the deletion must be submitted upon request.

- 9.5. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, insbesondere aus Aufbewahrungsverpflichtungen aus Unionsrecht oder dem für den Auftragnehmer geltendem nationalen Recht folgen, sind durch den Auftragnehmer über die Beendigung der Vereinbarung hinaus aufzubewahren. Der entsprechende Zeitraum bestimmt sich nach den entsprechenden Aufbewahrungsfristen. Der Auftragnehmer kann sie zu seiner Entlastung bei Beendigung der Vereinbarung dem Auftraggeber übergeben. Dies gilt für die Rückgabe überlassener Datenträger und Equipment analog.
- 9.6. Der Auftragnehmer ist verpflichtet, ein Löschkonzept vorzuhalten und unmittelbar sicherzustellen, dass die Rechte auf Auskunft und auf Berichtigung sowie, soweit aufgrund datenschutzrechtlicher Bestimmungen vorgeschrieben, auf Vergessenwerden und Datenportabilität erfüllt werden können, es sei denn die Parteien haben dies ausdrücklich und schriftlich vom Leistungsumfang ausgeschlossen.
- 9.7. Entstehen nach Vertragsbeendigung oder dem Ende einer Onlineumfrage im Rahmen eines laufenden Hauptvertrags zusätzliche Kosten durch die Herausgabe oder Löschung der Daten, so trägt der Auftraggeber die hierdurch entstehenden Kosten, sofern und soweit es sich um Daten des Auftragsverhältnisses handelte, die er selbst löschen konnte. Die Parteien dieser Vereinbarung sind sich darüber einig, dass der Auftraggeber alle im Rahmen einer Onlineumfrage übermittelten oder erhobenen personenbezogenen Daten selbst in der zur Verfügung gestellten Software-as-a-Service-Lösung direkt löschen kann. Eine eventuelle Verlängerung der Aufbewahrungsdauer aufgrund von Sicherheitskopien (Backups) ist dem Löschkonzept des Auftragnehmers zu entnehmen.

## 10. Subunternehmer

- 10.1. Der Auftragnehmer nimmt zurzeit folgende weitere Auftragsverarbeiter als Subauftragnehmer in Anspruch:
- SpaceNet AG (VPS-Hosting Webserver)  
Joseph-Dollinger-Bogen 14, 80807 München
  - Hetzner Online GmbH (Datensicherung)  
Industriestr. 25, 91710 Gunzenhausen
  - LOX24 GmbH (Versand von SMS)  
Seestraße 109, 13353 Berlin
- 10.2. Zum Zeitpunkt des Abschlusses dieser Vereinbarung sind die vorstehenden aufgeführten Unternehmen als Unterauftragnehmer für Teilleistungen für den

All documents which serve as proof for correct and due data processing, in particular those resulting from data retention obligations under the law of the European Union or national law applicable to the Processor shall be retained by the Processor beyond the termination of this agreement. The relevant period is determined by the corresponding data retention period. He may hand them over to the Controller for his exoneration upon termination of the agreement. The above mentioned applies accordingly to the return of transferred data carriers and equipment.

The Processor is obliged to maintain a deletion concept and to ensure immediately that the right to access, information and rectification as well as the right to be forgotten and for data portability, insofar as prescribed by data protection regulations, can be fulfilled, unless the parties have expressly excluded these rights from the contract in writing.

If additional costs arise after the termination of the contract or after the end of an online survey within the framework of a running main contract due to necessary handover or deletion of data, the Controller shall bear these costs if and to the extent that the data concerned was part of the contractual relationship, which he was able to delete himself. The parties to this agreement declare and understand that the Controller may directly delete all personal data transferred or collected as part of an online survey in the provided Software-as-a-Service solution. A possible prolongation of the retention period due to backup measures can be found in the deletion concept of the Processor.

## Subcontractors

The Processor currently accepts the following further processors as subcontractors:

- SpaceNet AG (VPS hosting web server)  
Joseph-Dollinger-Bogen 14, 80807 München
- Hetzner Online GmbH (data backup)  
Industriestr. 25, 91710 Gunzenhausen, Germany
- LOX24 GmbH (sending SMS)  
Seestr. 109, 13353 Berlin, Germany

At the time of the entering into this agreement, the above listed companies are subcontractors for certain services for the Processor and process and / or

Auftragnehmer tätig und verarbeiten und/oder nutzen in diesem Zusammenhang auch unmittelbar die Daten des Auftraggebers. Für diese Unterauftragnehmer gilt die Einwilligung für das Tätigwerden als erteilt. Eine Datenübermittlung in ein Drittland findet hierdurch nicht statt.

- 10.3. Der Auftragnehmer ist berechtigt, weitere Unterauftragnehmer hinzuzuziehen oder die in Anspruch genommenen Unterauftragnehmer durch andere Unterauftragnehmer zu ersetzen. Der Auftragnehmer informiert den Auftraggeber jedoch vorab über die beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung. Der Auftraggeber kann gegen die beabsichtigte Änderung Widerspruch erheben. Der Widerspruch ist innerhalb einer Ausschlussfrist von vier Wochen ab Erhalt der Information über die beabsichtigte Änderung zu erheben. Sowohl die Information als auch der Widerspruch bedürfen der Textform, wobei der Auftragnehmer den Auftraggeber in der Information noch einmal auf die Ausschlussfrist hinweisen wird. Erhebt der Auftraggeber ohne wichtigen Grund Widerspruch gegen die Änderung, ist der Auftragnehmer mit einer Frist von vier Wochen zur vorzeitigen Kündigung sowohl dieses Vertrages als auch des Hauptvertrages berechtigt.
- 10.4. Die Beauftragung von Auftragnehmern/Subunternehmern außerhalb der EU/des EWR wird ausgeschlossen. Der Auftragnehmer stellt sicher, dass sich die Rechenzentren aller Auftragnehmer/Unterauftragnehmer, in welchen personenbezogene Daten verarbeitet werden, in der/dem EU/EWR befinden.
- 10.5. Der Auftragnehmer wird den Unterauftragnehmern im Wege eines Vertrages dieselben Datenschutzpflichten auferlegen, die in diesem Vertrag zwischen den Parteien festgelegt sind.
- 10.6. Dienstleistungen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Durchführung der AVV in Anspruch nimmt, stellen keine Subunternehmerverhältnisse im Sinne dieser Regelung dar. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte oder Prüfer. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten den Auftraggeber auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

## 11. Besondere Vorschriften bei Fernwartung

Folgende Bestimmungen und ergänzende Vorgaben

directly use the Controller's data in this context. For these subcontractors, the consent for involvement is hereby considered granted. A data transfer to a third country does hereby not take place.

The Processor shall be entitled to involve further subcontractors or to replace the subcontractors claimed with other subcontractors. However, the Processor shall inform the Controller in advance of the intended change with regard to the involvement or replacement. The Controller may object against the intended change. The objection must be raised within a preclusive period of four weeks from the day of the receipt of the information about the intended change. Both, the information as well as the objection require text form, whereby the Processor will again point out the preclusive period to the Controller in his information. If the Controller raises an objection against the change without good cause, the Processor shall be entitled to terminate this Agreement and the underlying main contract prematurely with a notice period of four weeks.

The assignment of contractors/subcontractors outside the EU/EEA is excluded. The Processor must ensure that the data centers of all contractors/subcontractors are located in the EU/EEA, if personal data is handled in these data centers.

The Processor shall by way of agreement oblige the subcontractors to comply with the same data protection obligations as are set out in this agreement between the parties.

Services which the Processor makes use of with third parties as an ancillary service in order to assist in the performance of the DPA shall not constitute subcontractor relationships within the meaning of the provision of this agreement. These include, for example, telecommunications services, maintenance and user service, cleaners or auditors. However, the Processor is obliged to ensure the protection and security of the data, to make appropriate contractual agreements in accordance with the Data Protection Laws, as well as to take control measures, even in case of externally awarded ancillary services.

## Specific Regulations for Remote Maintenance

The following provisions and supplementary speci-



finden Anwendung im Falle eines Fernwartungszugriffs durch den Auftragnehmer, sofern und soweit dies für die Vertragserfüllung der Nutzungsvereinbarungen oder dieses AVV erforderlich ist oder erforderlich werden kann.

- 11.1. Fernwartungsarbeiten dürfen nur mit Genehmigung des Auftraggebers erfolgen. Fernwartung erfolgt dergestalt, dass der Auftraggeber dem Auftragnehmer für ein Befragungsprojekt im Rahmen der Software des Auftragnehmers Verwaltungszugriff einräumt. Ein Fernwartungszugriff des Auftragnehmers auf Datenverarbeitungsanlagen des Auftraggebers selbst erfolgt hierbei nicht.
- 11.2. Die Fernwartung ist mindestens durch die gleichen Sicherheitsmaßnahmen (Benutzername und Passwort, verschlüsselte Datenübertragung) geschützt wie der Zugriff des Auftraggebers auf das Befragungsprojekt.
- 11.3. Dem Auftragnehmer werden durch den Auftraggeber Zugriffsrechte eingeräumt, die dieser zur Durchführung der Fernwartungsarbeiten tatsächlich benötigt. Der Auftraggeber stellt sicher, dass der Auftragnehmer nur insoweit auf gespeicherte personenbezogene Daten zugreifen kann, als dies zur Durchführung der Fernwartungsarbeiten unerlässlich notwendig ist.
- 11.4. Der Auftragnehmer darf von den ihm eingeräumten Zugriffsrechten nur insoweit für die Durchführung der Fernwartungsarbeiten unerlässlich notwendigen Gebrauch machen.
- 11.5. Der Auftraggeber ist berechtigt, die Fernwartungsarbeiten von einem Kontrollbildschirm aus zu verfolgen und jederzeit abzubrechen. Soweit der Auftragnehmer daran mitwirken muss, gewährleistet er, dass dies möglich ist.

## 12. Haftung

- 12.1. Auftraggeber und Auftragnehmer haften für den Schaden, der durch eine nicht den Datenschutzgesetzen entsprechende Verarbeitung verursacht wird, gemeinsam im Außenverhältnis gegenüber dem jeweils Betroffenen. Der Auftragnehmer haftet dabei ausschließlich für Schäden, die auf einer von ihm durchgeführten Verarbeitung beruhen, bei der
  - er den aus den Datenschutzgesetzen resultierenden und speziell für Auftragsverarbeiter auferlegten Pflichten nicht nachgekommen ist oder
  - er unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers handelte oder
  - er gegen die rechtmäßig erteilten Anweisungen

cations shall apply in the event of remote maintenance access by the Processor, insofar as and to the extent that this is or may become necessary for the performance of the purchase orders or this DPA.

Remote maintenance work may only be carried out with the approval of the Controller. Remote maintenance shall be conducted in such a way that the Controller grants the Processor administrative access for a survey project within the framework of the Processor's software. The Processor will hereby not have remote maintenance access to the Controller's own data processing systems.

Remote maintenance is protected at least by the same security measures (username and password, encrypted data transmission) as the Controller's access to the survey project.

The Processor shall be granted access rights by the Controller which the Processor actually needs to carry out the remote maintenance work. The Controller shall ensure that the Processor can only access stored personal data to the extent that this is indispensable for carrying out the remote maintenance work.

The Processor may make use of the access rights granted to him only to the extent that they are indispensable for carrying out the remote maintenance work.

The Controller is entitled to monitor the remote maintenance work from a control screen and to interrupt it at any time. As far as the Processor has to participate, he guarantees that this is possible.

## Liability

The Controller and the Processor shall be jointly liable to the data subject for any damage caused by processing that does not comply with the Data Protection Laws. The Processor shall be liable exclusively for damage resulting from processing carried out by him in which

he has not complied with the obligations resulting from the Data Protection Laws and which are imposed especially on him as processors, or

- he acted by disregarding instructions lawfully given by the Controller, or
- he has acted contrary to the instructions lawfully

des Auftraggebers gehandelt hat.

- 12.2. Kommt ein weiterer Auftragsverarbeiter (Subunternehmer) seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters (Subunternehmers).
- 12.3. Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff auf den Auftragnehmer vorbehalten. Im Innenverhältnis zwischen Auftraggeber und Auftragnehmer haftet der Auftragnehmer für den durch eine Verarbeitung verursachten Schaden jedoch nur, wenn er
- seinen ihm speziell durch die DSGVO auferlegten Pflichten nicht nachgekommen ist oder
  - unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers oder gegen diese Anweisungen gehandelt hat.
- 12.4. Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt.

### 13. Kosten

- 13.1. Der Auftragnehmer erbringt die Umsetzung der durch die Nutzungsvereinbarungen festgelegten Weisungen und sorgt für die Einhaltung der allgemeinen und technischen und organisatorischen Maßnahmen, ohne dem Auftraggeber dafür Kosten nach diesem Vertrag zu berechnen. Insoweit sind die Tätigkeiten des Auftragnehmers also schon durch die Vergütung nach Maßgabe des Hauptvertrages abgegolten. Das gleiche gilt für Einzelweisungen, die der Auftraggeber über das Verarbeitungssystem des Auftragnehmers nach den Nutzungsvereinbarungen selbst umsetzen kann und auch selbst umsetzt (bspw. eigene Löschungspflicht von Daten gemäß Ziffer 9.3).
- 13.2. Dagegen fallen Kosten für die Umsetzung von Einzelweisungen und sonstiger Verlangen, welche über den Regelbetrieb hinausgehen beziehungsweise nicht Gegenstand des Hauptvertrags sind, dem Auftraggeber zur Last. Dies gilt insbesondere für die Unterstützung bei der Beantwortung von Betroffenenanträgen und bei der Einhaltung sonstiger Pflichten, die dem Auftraggeber obliegen, für die Rückgabe und Vernichtung von Daten entsprechend Ziffer 9.7, soweit diese über eine Löschung im System des Auftragnehmers hinausgeht, für die Zurverfügungstellung von Informationen, soweit diese nicht überwiegend im Interesse des Auftragnehmers liegt, und für das Ermöglichen und Beitragen zu Prüfungen einschließlich Inspektionen, soweit diese über eine ver-

given by the Controller.

If another processor (subcontractor) fails to comply with its data protection obligations, the Contractor shall be liable to the Controller for compliance with the obligations of that other processor (subcontractor).

Insofar as the Controller is obliged to pay indemnification to the party concerned, he reserves the right to rely on the Processor. In the internal situation between the Controller and the Processor, the Processor is only liable for the damage caused by processing, however, if the Processor

- has not complied with its obligations especially imposed on him by the GDPR
- acted in disregard of or against the instructions lawfully given by the Controller.

Any further liability claims according to the general laws remain unaffected.

### Expenses

The Processor shall implement the instructions specified in the purchase orders and shall ensure compliance with the general and also the technical and organizational measures without charging the Controller costs in accordance with this contract. Insofar the services of the Processor are already covered by the remuneration in accordance with the main contract. The same applies to individual instructions which the Controller can execute himself via the processing system of the Processor in accordance with the purchase orders (e.g. own obligation to delete data in accordance with Section 9.3).

Conversely, costs for the implementation of individual instructions and other requests, exceeding the regular operation or not being subject of the main contract, shall be charged to the Controller. This applies in particular for assistance services provided for responding to claims and for the fulfillment of other obligations imposed on the Controller for the return and destruction of data according to Section 9.7, insofar as this goes beyond erasure in the Processor's system, for the providing of information, insofar as this is not mainly in the Processor's interest, and to enabling and contributing to audits, including inspections but only to the extent, that these inspections do not exceed reasonable and appropriate measures. There shall be no obligation to bear the costs

hältnismäßige Prüfung beim Auftragnehmer hinausgehen. Eine Pflicht zur Kostentragung besteht nicht, wenn die Unterstützung wegen eines Gesetzes- oder Vertragsverstoßes des Auftragnehmers erforderlich wurde.

- 13.3. Auf Verlangen wird der Auftragnehmer dem Auftraggeber vorab eine Kostenschätzung geben. Zu den Kosten gehört auch eine angemessene Vergütung des Arbeitsaufwands. Der Stundensatz beträgt **150 € zzgl. USt.** Abweichende Kostenregelungen aus den Nutzungsvereinbarungen oder einer in den Nutzungsvereinbarungen einbezogenen Preisliste, die sich auf datenschutzrechtliche Maßnahmen beziehen, gehen dieser Kostenregelung vor. Ebenso fallen die Kosten für Maßnahmen, deren Erforderlichkeit eine Partei schuldhaft verursacht hat, dieser Partei zur Last. Ein Mitverschulden der jeweils anderen Partei ist jedoch zu berücksichtigen.

#### 14. Vertragsbeendigung, Schlussbestimmungen

- 14.1. Unbeschadet sonstiger Bestimmungen des Vertrags, insbesondere Ziffer 2.4, ist der Auftraggeber berechtigt, die jeweiligen Nutzungsvereinbarungen und diesen AVV jederzeit ohne Einhaltung einer Frist zu kündigen, wenn der Auftragnehmer schwerwiegend gegen eine Bestimmung dieses AVV verstößt, eine datenschutzrechtliche Weisung gemäß Ziffer 5 dieses AVV nicht umsetzt oder Kontrollen des Auftraggebers gemäß vorstehender Ziffer 6 dieses AVV verweigert.
- 14.2. Weisungen des Auftraggebers, die als wesentliche Vertragsänderungen durch den Auftraggeber zu verstehen sind, insbesondere aber nicht abschließend bei einer Weisung entsprechend der Regelung in Ziffer 5.4, ist der Auftragnehmer seinerseits zur außerordentlichen Kündigung dieses AVV wie des zugrundeliegenden Hauptvertrags berechtigt.
- 14.3. Sollten die Daten des Auftraggebers bei dem Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder vergleichbare Verfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlichem im Sinne der Datenschutzgrundverordnung liegen.
- 14.4. Änderungen, Ergänzungen und die Aufhebung dieses AVV müssen in dokumentierter Form erfolgen. Dies gilt entsprechend für die Änderung dieser Formklausur

if the assistance became necessary due to a breach of law or a breach of contract by the Processor.

Upon request, the Processor shall provide the Controller with a cost estimate in advance. The costs shall also include reasonable remuneration for the work involved. The hourly rate is **150 € plus VAT**. Deviating cost regulations from the purchase orders or a price list included in the purchase orders, which refer to data protection measures, shall prevail over these cost regulations. Likewise, the costs of measures whose necessity a party has culpably caused shall be charged to that party. However, any contributory negligence of the other party shall hereby be considered.

#### Termination of the contract, final provisions

Notwithstanding any other provisions of this agreement, in particular section 2.4, the Controller shall be entitled to terminate the applicable purchase order and this DPA at any time without notice if the Processor seriously violates any provision of this DPA, fails to implement a data protection instruction pursuant to section 5 of this DPA or refuses to inspections through the Controller pursuant to section 6 of this DPA.

In the event of instructions by the Controller which are to be understood as material contractual amendments by the Controller, in particular but not limited to an instruction in accordance with the provision in section 5.4, the Processor shall be entitled to terminate this DPA for good cause in the same way as the underlying main contract.

Should the Controller's data be endangered by seizure or confiscation by the Processor, by insolvency or comparable proceedings or by other events or measures of third parties, the Processor shall immediately inform the Controller thereof. The Processor shall immediately inform all persons responsible in this context that the sovereignty and ownership of the data lies exclusively with the Controller as the responsible authority within the meaning of the GDPR.

Amendments, supplements and termination of this DPA shall be made in a documented form. This shall apply accordingly to the amendment of this form

sel. Dokumentierte Form im Sinne dieses Vertrages meint mindestens die Textform. Auf Verlangen einer Partei ist eine in Textform abgegebene Erklärung schriftlich zu bestätigen.

- 14.5. Die englische Version dieser Vereinbarung verstehen die Parteien nur als unverbindliche Übersetzung. Im Falle von Widersprüchen ist die deutsche Version maßgeblich.

clause. Documented form in the understanding of this contract means at least text form. At request of any party, a declaration made in text form shall be confirmed in writing.

The English version of this agreement solely serves as convenient translation. In case of contradictions, the German version shall prevail.

Für den Auftraggeber / For the Controller

Ort, Datum  
Place, Date

Name und Position in Blockschrift  
Name and position in block capitals

Unterschrift, ggf. Stempel  
Signature, if applicable stamp

Für den Auftragnehmer / For the Processor

München, den 03.05.2026

Dr. Dominik Leiner, Geschäftsführer

Unterschrift  
Signature

## Anlagen

zu dieser Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag.

**Anlage 1:** Art und Zweck der Auftragsverarbeitung

**Anlage 2:** Verpflichtungserklärung

**Anlage 3:** Technische und organisatorische Maßnahmen des Auftragnehmers (TOM)

## Annexes

to this agreement on the processing of personal data for the controller

**Annex 1:** Type and purpose of contract processing

**Annex 2:** Declaration of commitment

**Annex 3:** Technical and Organizational Measures of the Contractor (TOM)

**Example – please provide the correct categories of data subjects and data under [s2survey.net/DSGVO/](https://s2survey.net/DSGVO/)**

### Anlage 1

#### Art und Zweck der Daten und Verarbeitung

#### 1. Art der vertragsgegenständlichen Daten, die der Auftragnehmer verarbeitet:

- Namen
- Verbindungsdaten (u.a. Zeitpunkt des Fragebogen-Aufrufs)
- Kommunikationsdaten (E-Mail-Adressen, Telefon-

### Annex 1

#### Nature and purpose of the data and processing

#### Type of data subject which the Processor processes:

- Names
- Connection data (including the time of the questionnaire access)
- Communication data (email addresses, telephone

nummern)

- Interessen
- Konsum-, Kommunikations- und Alltagsverhalten
- Unternehmenszugehörigkeit und Positionen im Unternehmen

numbers)

- Interests
- Consumption, communication and everyday behavior
- Company affiliation and positions in the company

## 2. Kategorien von der Verarbeitung betroffener Personen:

- Mitarbeiter des Auftraggebers
- Lieferanten des Auftraggebers

## Categories of data subjects to be processed:

- Employees of the responsible party
- Addressees of the survey (if they do not take part in the survey, only their contact details will be processed)
- Lieferanten des Auftraggebers

## 3. Art und Zweck der Auftragsverarbeitung

- 3.1. Umfang, Art und Zweck der Aufgaben des Auftragnehmers in Bezug auf den Auftragsgegenstand ergeben sich aus den Nutzungsvereinbarungen i.V.m Ziffer 1.1. vorstehender AVV:

Bereitstellung der Softwarelösung SoSci Survey als Software-as-a-Service-Lösung (Cloud Service), die Umfragebetreiber bei der professionellen Durchführung ihrer Onlinebefragung unterstützt, indem diese

- die Erstellung von Onlinefragebögen ermöglicht,
- Einladungen sowie ggf. Nachfassaktionen versendet und
- Datendownload der Umfrageergebnisse ermöglicht.

- 3.2. Sofern in der jeweiligen Nutzungsvereinbarung keine individuelle Datenauswertung vereinbart wurde, ist Art, Umfang und Zweck dieser AVV ist nicht die originale Nutzung oder Verarbeitung von personenbezogenen Daten durch den Auftragnehmer. Der Auftragnehmer stellt eine Infrastruktur (Cloud-Dienstleistung) zur Verfügung, welche dem Auftraggeber die Eingabe und Erhebung von personenbezogenen Daten und deren weitere Verarbeitung auf Systemen des Auftragnehmers ermöglicht.

Im Zuge der Leistungserbringung, insbesondere der Wartung, kann jedoch nicht ausgeschlossen werden, dass Mitarbeiter des Auftragnehmers Kenntnis von personenbezogenen Daten erhalten.

## Nature and purpose of the processing

The scope, nature and purpose of the Controller's tasks regarding the subject matter of the contract are set out in the purchase orders in accordance with section 1.1 of the above DPA:

Provision of the software SoSci Survey as a software-as-a-service solution (Cloud Service) which provides support to survey creators in the professional performance of their online surveys by providing them with

- the opportunity to create online questionnaires,
- invitations and, if necessary, follow-up actions, and
- data download of the survey results.

Unless an individual data analysis has been agreed in the the applicable purchase order, the nature, scope and purpose of these DPA is not primary the use or processing of personal data by the Processor. The Processor shall provide an infrastructure (cloud service) which enables the Controller to enter and collect personal data and to process them further on systems of the Processor.

However, access to personal data is not completely impossible during the performance of the Processor as a service provider while providing online survey services.

## 4. Dauer der Datenverarbeitung

Die Dauer der Bearbeitung wurde in der jeweiligen Nutzungsvereinbarung vereinbart.

## Duration of the processing

The duration of the processing has been agreed in the applicable purchase order.

## **Anlage 2**

### **Verpflichtungserklärung**

#### **1. Verpflichtungserklärung nach der Datenschutzgrundverordnung (nachfolgend „DSGVO“ genannt)**

Über die Bedeutung und die Vorschriften der DSGVO und des Bundesdatenschutzgesetzes (nachfolgend „BDSG n.F.“ genannt) ist der Auftragnehmer informiert. Danach ist es dem Auftragnehmer untersagt – unbeschadet sonstiger Geheimhaltungsverpflichtungen – unbefugt personenbezogene Daten, die dem Auftragnehmer aufgrund seines Vertragsverhältnisses und/oder im Zusammenhang mit seinem Vertragsverhältnis bekannt sind oder noch bekannt werden, zu verarbeiten (Verschwiegenheitspflicht nach Art. 28 Abs. 3 lit. b DSGVO). Die Verschwiegenheitspflicht gilt für sämtliche personenbezogene Daten, die durch den Auftraggeber und/oder die mit dem Auftraggeber gemäß §§ 15ff. Aktiengesetz (nachfolgend „AktG“ genannt) verbundenen Unternehmen verarbeitet werden. Zur Einhaltung dieser Verschwiegenheitspflicht verpflichtet sich der Auftragnehmer mit seiner Unterschrift.

#### **2. Verpflichtungserklärung nach dem Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (nachfolgend „TDDDG“ genannt)**

Über die Bedeutung und die Vorschriften des TDDDG zur Vertraulichkeit der Kommunikation (Fernmeldegeheimnisses) ist der Auftragnehmer informiert. Danach ist es dem Auftragnehmer untersagt, sich oder anderen über das für die Erbringung der Telekommunikationsdienste oder für den Betrieb ihrer Telekommunikationsnetze oder ihrer Telekommunikationsanlagen einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder von den näheren Umständen der Telekommunikation zu verschaffen. Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, dürfen nur aufgrund einer gesetzlichen Vorschrift oder einer ausdrücklichen Einwilligung des oder der Betroffenen über das vorgenannte Maß hinaus verwendet und insbesondere an Dritte weitergegeben werden (gemäß § 3 TDDDG). Zur Einhaltung des Fernmeldegeheimnisses verpflichtet sich der Auftragnehmer mit seiner Unterschrift.

## **Annex 2**

### **Declaration of Commitment**

#### **Declaration of Obligation under the General Data Protection Regulation (hereinafter referred to as "GDPR")**

The Processor has been informed about the meaning and rules of the GDPR and the new version of the German Federal Data Protection Act (hereinafter referred to as "BDSG new version"). According to them, the Processor has been prohibited – notwithstanding other confidentiality obligations – from processing personal data of which he has or acquire knowledge on account of and/or in connection with my contractual relationship (Confidentiality Obligation under Art. 28 (3) letter b GDPR). The confidentiality obligation applies to all personal data that are processed by Principal and/or companies affiliated with Principal as defined by Sections 15 et seqq. of the German Stock Corporation Act (Aktiengesetz, hereinafter referred to as AktG). The Processor agrees to comply with this confidentiality requirement by signing the contract.

#### **Declaration of commitment pursuant to the Telecommunications Digital Services Data Protection Act (hereinafter referred to as "TDDDG")**

The processor is aware of the significance and provisions of the TDDDG regarding the confidentiality of communications (telecommunications secrecy). Accordingly, the processor is prohibited from obtaining knowledge of the content or details of telecommunications beyond what is necessary for the provision of telecommunications services or for the operation of its telecommunications networks or telecommunications equipment, including the protection of its technical systems. Knowledge of facts subject to telecommunications secrecy may only be used beyond the aforementioned extent and, in particular, passed on to third parties on the basis of a legal provision or the express consent of the person or persons concerned (in accordance with § 3 TDDDG). The contractor undertakes to comply with telecommunications secrecy by signing this agreement.



### 3. Geheimhaltung von vertraulichen Informationen

Unbeschadet des Vorgenannten verpflichtet sich der Auftragnehmer mit seiner nachstehenden Unterschrift, Informationen, die ihm bekannt sind oder werden, während des Vertragsverhältnisses weder unbefugt zu verwerten noch unbefugt Dritten mitzuteilen. Dritte sind auch Personen, die mit dem Auftraggeber und/oder mit dem Auftraggeber gemäß §§ 15ff. AktG verbundenen Unternehmen vertraglich verbunden sind, soweit diese nicht jeweils durch ihre Funktion und/oder Tätigkeit zur Entgegennahme derartiger Mitteilungen befugt sind, wobei unbefugt das Fehlen einer Rechtsgrundlage meint.

Vertrauliche Informationen sind insbesondere Geschäfts- und Betriebsgeheimnisse, Vertragsschlüsse, technische oder kaufmännische Informationen jedweder Art bzw. anderweitige Angaben, die als vertraulich bezeichnet oder ihrer Natur nach als vertraulich anzusehen sind. Diese Geheimhaltungspflicht erstreckt sich auf vertrauliche Informationen des Auftraggebers und/oder der mit dem Auftraggeber gemäß §§ 15ff. AktG verbundenen Unternehmen.

Der Auftragnehmer erklärt, dass er seine Mitarbeiter, die personenbezogene Daten des Auftraggebers verarbeiten, auf das Datengeheimnis und, sofern anwendbar, auf die ärztliche Schweigepflicht gem. § 203 Strafgesetzbuch verpflichtet hat. Die Mitarbeiter sind entsprechend geschult.

### 4. Reichweite und Dauer der Verpflichtungen sowie Hinweise auf Strafvorschriften

Die vorstehenden Verpflichtungen auf

- die Verschwiegenheit (Ziffer 1);
- das Fernmeldegeheimnis (Ziffer 2);
- die Geheimhaltung von vertraulichen Informationen (Ziffer 3)
- die ärztliche Schweigepflicht gem. § 203 StGB (Ziffer 3)

bestehen auch nach Beendigung des Vertragsverhältnisses fort, ungeachtet dessen, welche Ursachen der Beendigung des Vertragsverhältnisses zugrunde liegen.

Der Auftragnehmer ist sich bewusst, dass Zuwiderhandlungen gegen die DSGVO, die EDPR, das BDSG n.F. (gemäß § 42 BDSG n.F.), das Strafgesetzbuch (gemäß § 203, 206 Strafgesetzbuch, nachfolgend „StGB“ genannt) und das TDDDG sowie die Verletzung der

### Maintaining Secrecy of Confidential Information

Notwithstanding the aforementioned, the Processor hereby undertakes during the contractual relationship neither to utilize confidential information that is or becomes known to him nor to share it with third parties without authorization. Third parties include persons that are contractually tied to the Controller and/or to companies affiliated with the Controller as defined in Sections 15 et seqq. AktG, to the extent that they are not authorized by their function and/or activity to receive such communications whereby unauthorized means the absence of a legal basis.

Confidential information includes in particular commercial and operating secrets, contracts entered into, technical or commercial information of any kind or other information that is labeled as confidential or is to be viewed as confidential by nature. This duty to maintain secrecy extends to confidential information of the Controller and/or companies affiliated with the Controller as defined in Sections 15 et seqq. AktG.

The processor declares that it has obliged its employees who process the controller's personal data to maintain data confidentiality and, where applicable, medical confidentiality in accordance with Section 203 of the Criminal Code. The employees have been trained accordingly.

### Reach and Duration of the Obligations and References to Criminal Rules

The preceding obligations toward

- the confidentiality (Section 1);
- the privacy of telecommunications (Section 2);
- the maintenance of secrecy of confidential information (Section 3)
- Medical confidentiality pursuant to Section 203 of the German Criminal Code (StGB) (Section 3)

shall continue to exist after the end of the contractual relationship, regardless of the causes for the end of the contractual relationship.

The processor is aware that violations of the GDPR, the EDPR, the BDSG n.F. (in accordance with § 42 BDSG n.F.), the Criminal Code (in accordance with § 203, 206 of the Criminal Code, hereinafter referred to as “StGB”) and the TDDDG, as well as the violation

Geheimhaltungspflicht von vertraulichen Informationen nach verschiedenen Vorschriften, zivil- und strafrechtliche Folgen auslösen können.

Falls eine der vorstehenden Bestimmungen gesetzlichen und/oder sonstigen Bestimmungen widerspricht, wird hierdurch die Gültigkeit der übrigen Bestimmungen dieser Verpflichtungserklärung auf das Daten- und Fernmeldegeheimnis sowie die Geheimhaltung von vertraulichen Informationen nicht berührt.

Der Auftragnehmer erklärt mit seiner Unterschrift, die einschlägigen Gesetze, insbesondere DSGVO, EDPR, BDSG n.F., TDDDG, StGB und UWG zu beachten. Ein Duplikat dieser von ihm unterzeichneten Verpflichtungserklärung, die sowohl ihn persönlich als auch die Gesellschaft, für die er handelt verpflichtet, hat er zu den Unterlagen genommen und erklärt weiterhin mit seiner Unterschrift, für ihn tätige Mitarbeiter entsprechend verpflichtet zu haben.

of the duty of confidentiality of confidential information under various regulations, may result in civil and criminal consequences.

If any of the above provisions contradicts legal and/or other provisions, this shall not affect the validity of the remaining provisions of this Declaration of Obligation toward the privacy of data and telecommunications and toward the maintenance of secrecy of confidential information.

By signing this document, the processor declares that it will comply with the relevant laws, in particular the GDPR, EDPR, BDSG (new version), TDDDG, StGB, and UWG. A duplicate of this declaration of commitment signed by him, which is binding on both him personally and the company for which he acts, has been added to the documents, and he further declares with his signature that he has bound employees working for him accordingly.

München, den 03.05.2026

---

Dr. Dominik Leiner

(für sich persönlich wie in seiner Funktion als Geschäftsführer für die Gesellschaft handelnd)  
(acting for himself personally as well as in his role as Managing Director for the Company)

**Anlage 3**  
**Technische und organisatorische**  
**Maßnahmen des Auftragnehmers (TOM)**  
Stand vom 03.05.2026

**Rahmeninformation**

Die Verarbeitung der personenbezogenen Daten erfolgt im Regelfall auf den technischen Anlagen eines Subunternehmers (Webhoster). Die technischen Anlagen (Webserver) des Subunternehmers sind in einem nach ISO 27001 zertifizierten Rechenzentrum untergebracht. Für diese Unterbringung (Housing) kann der Webhoster optional auf die Leistungen eines weiteren Unternehmens (Betreiber des Re-

**Annex 3**  
**Technical and Organizational Measures**  
**of the Processor (TOM)**  
Status as of 03.05.2026

**Background information**

Personal data is generally processed on the technical infrastructure of a subcontractor (web host). The subcontractor's technical infrastructure (web servers) is housed in a data center certified to ISO 27001. For this housing, the web host may optionally rely on the services of another company (the data center operator), which, however, is not a subcon-

chenzentrums) zurückgreifen, welches allerdings kein Subunternehmer im Sinne der DSGVO ist. Zum aktuellen Zeitpunkt erfolgt der Betrieb des Rechenzentrums (Housing) durch den Webhoster.

- Bei Nutzung des Befragungsservers **s2survey.net** findet im Regelfall keine Verarbeitung auf den Anlagen des Auftragnehmers statt.
- Die Nutzung des Befragungsservers **www.soscisurvey.de** ist nicht Gegenstand des vorliegenden Dokuments.

Eine über den Regelfall hinausgehende Übermittlung oder andere Verarbeitung der Daten auf die/den Anlagen des Auftragnehmers findet nur auf schriftliche Weisung des Auftraggebers hin statt, etwa um unschlüssige technische oder inhaltliche Sachverhalte zu klären. Die dabei ergriffenen technischen und organisatorischen Maßnahmen sind in der folgenden Darstellung enthalten.

Ein großer Teil der technischen Maßnahmen zum Schutz der verarbeiteten Daten, insbesondere der physische Zugriff auf die Anlagen, ergibt sich daher aus den technischen und organisatorischen Maßnahmen (TOM) des Webhosters, welche dem Verarbeiter vorliegen und auf Anfrage eingesehen werden können. Die folgenden Dokumente werden nachfolgende zitiert:

- Hosting Befragungsserver: Technische und organisatorische Maßnahmen (TOM) der SpaceNet AG vom 12.05.2025 (v1.8).
- Hosting Datensicherung: Technische und organisatorische Maßnahmen (TOM) der Hetzner GmbH vom 16.02.2026 (Produkt "Cloud Server", v1.2).

tractor within the meaning of the GDPR. At this time, the data center (housing) is operated by the web hosting provider.

- When using the **s2survey.net** survey server, no processing usually takes place on the processor's systems.
- The use of the survey server **www.soscisurvey.de** is not the subject of this document.

Any transfer or other processing of the data to the processor's system(s) that goes beyond the normal case shall only take place on the written instruction of the Controller, for example in order to clarify inconclusive technical or content-related issues. The technical and organizational measures taken in this connection are contained in the following description.

A large part of the technical measures for protecting the processed data—particularly regarding physical access to the facilities—therefore stems from the web host's technical and organizational measures (TOM), which are available to the processor and can be viewed upon request. The following documents are cited below:

- Survey server hosting: Technical and organizational measures (TOM) of SpaceNet AG dated 12.05.2025 (v1.8).
- Data backup hosting: Technical and organizational measures (TOM) of Hetzner GmbH dated 16.02.2026 (product "Cloud Server", v1.2).

## 1. Vertraulichkeit

### 1.1. Zutrittskontrolle

#### Hosting Befragungsserver (SpaceNet, 2025, S. 11)

- Der Webhoster hat ein Security Management System (ISMS) eingerichtet,
- Zutrittskontrollsystem mit Protokollierung
- Die Schlüsselvergabe ist zentral und organisatorisch klar geregelt
- Klare Zuweisung der Berechtigungen
- Der Gebäudeschutz ist an Wochenenden und nachts gewährleistet
- Es bestehen Regelungen für Besucher

## Confidentiality

### Access Control Rooms

#### Hosting Survey Server (SpaceNet, 2025, p. 11)

- The web host has implemented an Information Security Management System (ISMS),
- Access control system with logging
- Key distribution is centrally managed and clearly regulated within the organization
- Clear assignment of access permissions
- Building security is ensured on weekends and at night
- Visitor policies are in place

- Videoüberwachung sensibler Bereiche des Gebäudes, innerhalb der Rechenzentrumsräume sind Kameras für jeden Gang installiert.
- Verschließen von Schränken und Büros bei Nichtanwesenheit in sensiblen Bereichen
  - Prüfung aller Mitarbeiter des Rechenzentrums und der Zugriffsebenen
  - Mitarbeiter-Lifecycle, in dem geregelt ist, welche Personenkreise Zugang zum Rechenzentrum erhalten. Abweichungen hiervon müssen durch den CISO genehmigt werden.
- Der gesamte Zugriff auf das Rechenzentrum wird protokolliert und überwacht.

#### Hosting Datensicherung (Hetzner, 2026, S. 1)

- Elektronisches Zutrittskontrollsystem mit Protokollierung
- Dokumentierte Vergabe von Zutrittsmedien
- Flächendeckende Videoüberwachung
- Richtlinie zum Besuchermanagement
- Hochsicherheitszaun mit Übersteig- und Untergrabschutz um den gesamten Datacenter-Park
- Separierte Colocation-Bereiche mit abschließbaren Racks

## 1.2. Zugangskontrolle

Sämtliche Datenverarbeitungssysteme (sowohl lokal wie auch die eingesetzten Befragungsserver) sind mittels Passwörtern gesichert.

#### Auftragnehmer

Mindeststandards für Passwörter

- Unterschiedliche Zeichenzusammensetzung
- Mindestlänge 16 Zeichen
- Zugangssperre bei mehr als 3 Anmeldeversuchen

Verwaltung der Passwörter

- Etablierte Open Source Software
- Schutz des Zugriffs durch 2-Faktor Authentifizierung

#### Befragungsserver

Auf Software und Konfiguration basierende Zugangskontrollen:

Verwendete Server-Software

- Gängige Linux-Distribution (Open Source)
- Gängige Webserver-Anwendungen (Open Source)

Beschränkung von Server-Zugriffen

- Video surveillance of sensitive areas of the building; cameras are installed in every aisle within the data center rooms.
- Locking cabinets and offices when unattended in sensitive areas
  - Verification of all data center employees and their access levels
  - An employee lifecycle policy that specifies which groups of people are granted access to the data center. Any deviations from this policy must be approved by the CISO.
- All access to the data center is logged and monitored.

#### Hosting Backup (Hetzner, 2026, S. p)

- Electronic access control system with logging
- Documented issuance of access credentials
- Comprehensive video surveillance
- Visitor management policy
- High-security fence with anti-climb and anti-dig features surrounding the entire data center park
- Separate colocation areas with lockable racks

## Access Control Data

All data processing systems (both local and the survey servers used) are secured by passwords.

#### Contractor

Minimum standards for passwords

- Different characters composition
- Minimum length 16 characters
- Access blocking after more than 3 login attempts

Password management

- Established open source software
- Access protection by means of 2-factor authentication

#### Survey Server

Access controls based on software and configuration:

Software used on the server

- Common Linux distribution (open source)
- Common web server applications (open source)

Restriction of server access

- Beschränkung auf notwendige Ports (HTTP, HTTPS, E-Mail) mittels interner Firewall (iptables)
- Die Fernwartung ist nur für ausgewählte IP-Adressen erreichbar.

#### Sicherheitsupdates

- Sicherheitsupdates werden automatisiert mehrmals täglich installiert.

#### Verschlüsselung

- Die Daten werden verschlüsselt gespeichert (data at rest encryption).

#### Hosting Befragungsserver (SpaceNet, 2025, S. 12)

- Sollten shared LogOns oder Accounts zum Einsatz kommen, so werden die Verwendung protokolliert und können derjenigen Person zugeordnet werden, die diesen Account verwendet hat.
- Dezidiertes Kennwortverfahren zum Login (Passwortrichtlinie). Passwörter müssen regelmäßig geändert werden.
- Alle Logins, LogOffs und Fehler werden protokolliert.

#### Hosting Datensicherung (Hetzner, 2026, S. 2-3)

- Eigenes Kundenkonto mit zahlreichen Verwaltungsoptionen und Zugang zur Administrationsoberfläche
- Nachvollziehbare Protokollierung von Zugriffs- und Änderungsvorgängen im Kundenaccount
- Passwortpflicht für das Kundenkonto mit festgelegten Mindestanforderungen
- Option zur Zwei-Faktor-Authentifizierung (2FA) für Kundenkonto [wird genutzt]
- Serverzugriff erfolgt ausschließlich durch Auftraggeber (in diesem Fall die SoSci Survey GmbH)

#### Hosting Datensicherung (Hetzner, 2026, S. 8)

- Verpflichtungserklärung der Hetzner-Mitarbeitenden vor Tätigkeitsbeginn zur datenschutzkonformen Verarbeitung personenbezogener Daten
- Verpflichtungserklärung externer Personen vor Tätigkeitsbeginn zu Verschwiegenheit und Umsetzung von TOMs (bei Bedarf)
- Regelmäßige Sensibilisierungen und Schulungen der Hetzner-Mitarbeitenden bzgl. Datenschutz- und Informationssicherheitsthemen
- Verschlüsselungsoptionen für die Datenübertragung je nach Produktart unterschiedlich umge-

- Restriction to necessary ports (HTTP, HTTPS, e-mail) by means of internal firewall (iptables)
- The SSH management port is only accessible for selected IP addresses.

#### Security updates

- Security updates are installed automatically several times a day.

#### Encryption

- Data is stored in encrypted form (data at rest encryption).

#### Hosting Survey Server (SpaceNet, 2025, p. 12)

- If shared logins or accounts are used, their use is logged and can be traced back to the person who used the account.
- A strict password policy for logins (password policy). Passwords must be changed regularly.
- All logins, logouts, and errors are logged.

#### Hosting Backup (Hetzner, 2026, pp. 2-3)

- Dedicated customer account with numerous management options and access to the administration interface
- Comprehensive logging of access and modification activities within the customer account
- Password requirement for the customer account with specified minimum requirements
- Option for two-factor authentication (2FA) for the customer account [in use]
- Server access is granted exclusively to the client (in this case, SoSci Survey GmbH)

#### Hosting Backup (Hetzner, 2026, p. 8)

- Declaration of commitment by Hetzner employees prior to commencing work regarding the processing of personal data in compliance with data protection regulations
- Declaration of commitment by external parties prior to commencing work regarding confidentiality and the implementation of technical and organizational measures (TOMs) (as needed)
- Regular awareness campaigns and training for Hetzner employees on data protection and

setzt

information security topics

- Encryption options for data transmission implemented differently depending on the product type

### Verwaltungssysteme

Personenbezogene Daten werden im Regelfall nicht auf den Verwaltungssystemen oder externen/mobilen Medien gespeichert. Sollte dies im Aufnahmefall erforderlich werden, kommt eine Verschlüsselung nach dem PGP-Standard oder vergleichbar zum Einsatz (Schlüssellänge min. 3072 Bit).

Auf den Datenverarbeitungsanlagen des Verarbeiters wird eine Anti-Viren-Software eingesetzt, Sicherheitsupdates werden automatisiert installiert, die Internetverbindung erfolgt nur mittels NAT-Routing.

### Administrative systems

Personal data is stored on an external/mobile medium exclusively for the purpose of storing the backups described above. Encryption according to the PGP standard is used (key length min. 2048 bit).

Anti-virus software is used on the processor's data processing systems, security updates are installed automatically, the Internet connection is established via NAT router.

### 1.3. Zugriffskontrolle und Datenträgerkontrolle

Da nur die Geschäftsführer auf personenbezogene Daten zugreifen können, verzichtet die SoSci Survey GmbH auf ein detailliertes Rollenkonzept.

Die Verarbeitung der Daten erfolgt automatisiert, regelmäßig erfolgt kein Zugriff von Mitarbeitern oder Geschäftsführung auf die verarbeiteten Daten. Ein solcher Zugriff findet nur dann statt, wenn der Auftraggeber schriftlich darum bittet, etwa zur Klärung konkreter Sachverhalte.

Generell verwenden alle eingesetzten Systeme zeitlich Sperren:

- Auto-Logout/Bildschirmsperre
- Sperren nach ungültigen Anmeldeversuchen
- Zeitverzögertes Antwortverhalten bei Fehlversuchen

#### Hosting Befragungsserver (SpaceNet, 2025, S. 12)

- Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten.
- Autorisierungen werden schriftlich beantragt, ausschließlich durch das Management gewährt und protokolliert. Die Berechtigungen werden regelmäßig auf Aktualität überprüft.
- Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte.
- Jeder Mitarbeiter erhält nur diejenigen Zugriffsrechte, die für die Ausführung seiner Aufgaben er-

### Access Control and Media Control

Since only the managing directors have access to personal data, SoSci Survey GmbH does without a detailed role concept.

The processing of the data is automated, there is no regular access to the processed data by employees or management. Such access only takes place if the controller requests it in writing, for example to clarify specific facts.

In general, all systems use time locks:

- Auto-Logout/Screen lock
- Locking after invalid login attempts
- Delayed response behaviour in case of failed attempts

#### Hosting Survey Server (SpaceNet, 2025, p. 12)

- Prevention of unauthorized access to personal data, as well as unauthorized access to, alteration of, or deletion of stored personal data.
- Authorizations must be requested in writing, granted exclusively by management, and documented. Authorizations are regularly reviewed to ensure they remain up to date.
- Prevention of the use of automated processing systems by unauthorized persons using data transmission facilities.
- Each employee is granted only the access rights necessary to perform their duties (principle of least privilege).



forderlich sind (principle of least privilege).

- Es sind darüber hinaus Prozesse etabliert, die bei Eintritt, Abteilungswechsel oder Austritt eines Mitarbeiters u. a. den Umgang mit den Berechtigungen regeln („Mitarbeiter-Lifecycle“). Diese sind dokumentiert und werden protokolliert.
- Differenzierte Berechtigungen durch Profile und Rollen
- Richtlinie für mobile Geräte und Datenträger
- Richtlinie zur Sicherheit im Büro
- Sichere Löschung von Daten bzw. Vernichtung von Datenträgern.

#### Hosting Datensicherung (Hetzner, 2026, S. 4-5)

- Regelmäßige Sicherheitsupdates für zugrundeliegende Cloud-Infrastruktur
- Revisionssicheres, verbindliches Berechtigungsverfahren auf Basis eines Rollen- und Berechtigungskonzeptes für Zugriffe auf Cloud-Infrastruktur.
- Definiertes Verfahren zur Löschung von Festplattendaten nach Auftragsbeendigung (je nach Produktart unterschiedlich umgesetzt)
- Physische Zerstörung von Datenträgern bei nicht erfolgreicher Datenlöschung
- Physischer Zugriff auf Datenträger nur in definierten Bereichen; Transport standortübergreifend ausschließlich in verschlossenen Transportboxen

- In addition, processes are in place to govern, among other things, the management of access rights when an employee joins the company, changes departments, or leaves the company ("employee lifecycle"). These processes are documented and logged.
- Differentiated permissions based on profiles and roles
- Policy on Mobile Devices and Data Storage Media
- Office Security Policy
- Secure data deletion and destruction of data storage media.

#### Hosting Backup (Hetzner, 2026, pp. 4-5)

- Regular security updates for the underlying cloud infrastructure
- Audit-proof, binding authorization process based on a role- and permission-based model for access to the cloud infrastructure.
- Defined procedure for deleting hard drive data upon completion of the contract (implemented differently depending on the product type)
- Physical destruction of data storage media if data deletion is unsuccessful
- Physical access to data storage media is permitted only in designated areas; cross-site transport is permitted exclusively in locked transport boxes

## 1.4. Pseudonymisierung

### Pseudonymisierung von Befragungsdaten

Für den Fall, dass die Serienmail-Funktion von SoSci Survey verwendet und für die Adressaten ein anderer Datenschutz-Modus als „anonym“ eingestellt wurde, ist in der Datenbank ein Bezug zwischen erhobenen Daten und Adresseintrag hinterlegt. Sofern nicht der Datenschutz-Modus „personenbezogen“ für die Adresseinträge ausgewählt wurde, ist diese Zuordnung für den Auftraggeber nicht einsehbar – aus Sicht des Auftraggebers liegt eine effektive Pseudonymisierung vor.

### Anonymisierung von Befragungsdaten

Die Software-Funktion „Kontaktdaten getrennt erheben“ erlaubt die Abfrage und getrennte Speicherung einer E-Mail-Adresse oder anderer personenbezogener Daten (Adresseinträge) innerhalb eines Fragebogens. Die Speicherung erfolgt derart, dass (ab dem Vorliegen von mindestens zwei Datensätzen oder

## Pseudonymisation

### Pseudonymisation of Survey Data

In case the mailing feature of SoSci Survey is used and the data protection mode for the addressees is set to another mode than "anonymous", a reference between collected data and address entry is stored in the database. Unless the data protection mode "person-related" has been selected for the address entries, this reference is not visible to the controller – from the point of view of the controller, effective pseudonymisation is provided.

### Anonymization of Survey Data

The software feature "Collect Email Addresses Separately" allows an e-mail address or other personal data (address entries) to be queried and stored separately within a questionnaire. The storage takes place in such a way that (as soon as there are at least two data sets or at least two contact entries)

mindestens zwei Kontakteinträgen) eine Zuordnung einzelner Adresseinträge zu einzelnen Datensätzen der Befragung nicht mehr möglich ist.

it is no longer possible to relate individual address entries to individual data sets of the survey.

## 1.5. Trennungskontrolle

SoSci Survey ist ein Mehr-Mandantensystem, welches sowohl eingegebene als auch erhobene Daten innerhalb einer relationalen Datenbank grundsätzlich nach Befragungsprojekten trennt (interne Mandantenfähigkeit, interne Zweckbindung, Abschottung, Löschung).

Test-/Entwicklungs-System und Produktivsystem (Befragungsserver) laufen auf unterschiedlicher Hardware in unterschiedlichen Netzen, das Testsystem hat keinen Zugriff auf die Daten des Produktivsystems.

### Befragungsserver

- Durchgängige logische Partitionierung der Datenbank auf Ebene von Befragungsprojekten.
- Getrennte Speicherbereiche für hochgeladene Dateien auf Ebene von Befragungsprojekten.

Die Sicherung der Daten (Backup) erfolgt für den gesamten Befragungsserver (keine Differenzierung nach Befragungsprojekt/Mandant), Adressdaten (siehe „Anonymisierung von Befragungsdaten“) welche im Rahmen der Serienmail-Funktion eine Personenbeziehbarkeit erlauben, werden getrennt von den restlichen Daten gesichert.

### Hosting Befragungsserver (SpaceNet, 2025, S. 12)

- Physisch und/oder logisch getrennte Speicherung, Veränderung, Löschung und Übermittlung von Daten, die unterschiedlichen Zwecken dienen (insbesondere Trennung von Daten unterschiedlicher Kunden).
- Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.

### Hosting Datensicherung (Hetzner, 2026, S. 6)

- Physische oder logische Trennung von Daten
- Physische und logische Trennung von Backup-Daten

## Separation Control

SoSci Survey is a multi-client system that basically separates both entered and collected data within a relational database according to survey projects (internal multi-client capability, internal allocation).

Test-/development system and productive system (survey server) run on different hardware in different networks, the test system has no access to the data of the productive system.

### Survey Server

- Consistent logical partitioning of the database at the survey project level.
- Separate storage areas for uploaded files at the survey project level.

Data backups are performed for the entire survey server (without distinguishing between survey projects or clients); address data (see “Anonymization of Survey Data”) that could be linked to specific individuals when used with the mass email function is backed up separately from the rest of the data.

### Hosting Survey Server (SpaceNet, 2025, p. 12)

- Physically and/or logically separate storage, modification, deletion, and transmission of data used for different purposes (in particular, the separation of data belonging to different customers).
- Ensuring that personal data collected for different purposes can be processed separately.

### Hosting Backup (Hetzner, 2026, p. 6)

- Physical or logical separation of data
- Physical and logical separation of backup data

## 2. Integrität

## Integrity

### 2.1. Weitergabekontrolle

### Control of transfers

Alle Datentransporte erfolgen mittels Netzwerkübermittlung (verschlüsselte Datenübertragung), Datenträger kommen nicht zum Einsatz. Folgende Datentransporte finden Anwendung:

#### **Zugriffe auf das Web-Interface**

Die Übermittlung von Eingaben und erhobenen Daten zwischen dem Verarbeiter und dem Befragungsserver ist durch SSL-/TLS-Verschlüsselung geschützt. Auf dem Server s2survey.net kommt dafür ein Zertifikat mit Validierung (Organization Validation) zum Einsatz.

#### **Teilnahme an Befragungen**

Der Aufruf des Fragebogens und die Rückübermittlung von Daten des Befragten an den Befragungsserver ist durch SSL/TLS-Verschlüsselung geschützt.

#### **Verwaltungszugriffe auf den Befragungsserver**

Die Verwaltung des Befragungsservers sowie eventuelle Zugriffe auf die Datenbank erfolgen verschlüsselt mittels SSH (Datenzugriff via SSH-Tunnel).

Eine Fernwartung erfolgt, sofern erforderlich, ausschließlich durch den Auftragnehmer und den Hosting-Subunternehmer.

## **2.2. Eingabekontrolle**

Die Eingabe von Befragungsdaten erfolgt i.d.R. durch die Personen selbst, der Zeitpunkt der Dateneingabe ist Bestandteil der erhobenen Daten (Zeitstempel, Verweildauer). Eine zusätzliche Protokollierung für einzelne Befragungsprojekte kann optional in der Software aktiviert werden.

Da die Befragungsprotokolle Teil des Datensatzes sind, obliegt die Aufbewahrung dem Auftraggeber. Die Löschung der erhobenen Daten auf dem Befragungsserver geht mit einer Löschung der Metainformationen zur Befragung einher.

#### **Hosting Befragungsserver (SpaceNet, 2025, S. 13)**

- Die auf Servern erfolgenden Verwaltungstätigkeiten werden protokolliert, einschließlich der Login-History
- Protokollierungs- und Protokollauswertungssysteme werden eingesetzt bzw. sind als Teile von bestehenden Softwareapplikationen anwendbar
- Zugriff auf Datenverarbeitungssysteme nur nach Login möglich
- Keine Weitergabe von Passwörtern

All data transports are conducted via network transmission (encrypted data transmission), data carriers are not used. Data is transferred by using the following modes:

#### **Access to the Web Interface**

The transmission of input and collected data between the processor and the survey server is protected by SSL encryption. On the s2survey.net server a certificate with extended validation is used for this purpose.

#### **Participation in Surveys**

Access to the questionnaire and the return transmission of the respondent's answers to the survey server is protected by SSL encryption. On the server s2survey.net a certificate with extended validation is used for this purpose.

#### **Management access to the Survey Server**

The administration of the survey server as well as possible access to the database is encrypted via SSH (data access via SSH tunnel).

Remote maintenance, if necessary, is carried out exclusively by the hosting subcontractor.

## **Input control**

Survey data is usually entered by the persons themselves, the time of when the data is entered is part of the collected data (time stamp, survey duration). Additional logging for individual survey projects can be optionally activated in the software.

Since the survey protocols are part of the data set, the controller is responsible for keeping them. The deletion of the collected data on the survey server is accompanied by a deletion of the meta-information on the survey.

#### **Hosting Survey Server (SpaceNet, 2025, p. 13)**

- Administrative activities performed on servers are logged, including login history
- Logging and log analysis systems are used or are available as components of existing software applications
- Access to data processing systems is only possible after logging in
- Passwords must not be shared
- Workstations must be locked when leaving the

- Sperrung des Arbeitsplatzrechners beim Verlassen des Büros. office.

### 3. Verfügbarkeit und Belastbarkeit

#### Verfügbarkeitskontrolle

Der Betreiber des Rechenzentrums ist nach ISO 27001 zertifiziert.

Ein tägliches Disaster Recovery Backup wird durch den Hosting Subunternehmer erstellt und physisch getrennt aufbewahrt.

Ein zusätzliches tägliches, verschlüsseltes Backup zur Wiederherstellung versehentlich gelöschter Teildaten wird für den Zeitraum von 1 Monat (s2survey.net) bei einem separaten Hoster in einem separaten Rechenzentrum hinterlegt.

#### Hosting und Housing Befragungsserver (SpaceNet, 2025, S. 14)

- Alle Infrastrukturkomponenten, die der Auftragnehmer in den SpaceNet-Rechenzentren betreibt, sind an unterbrechungsfreie Stromversorgungssysteme sowie an eine Netzersatzanlage (Diesel-Generator) angeschlossen.
- Die Sicherung der Daten des Auftragnehmers erfolgen jeweils in ein entferntes Rechenzentrum des Auftragnehmers.
- Virenschutz ist auf allen Desktop- und Laptop-Rechnern im Netzwerk des Auftragnehmers vorgeschrieben. Es werden auf Netzwerkebene Angriffserkennungssysteme (IDS) eingesetzt, um eine Warnung vor etwaigen Angriffen zu erhalten.
- Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.
- Gewährleistung, dass eingesetzte Systeme im Störfall wiederhergestellt werden können.
- Regelmäßiges Backup-Verfahren ist gesichert
- Getrennte Aufbewahrung von produktiven Daten und Datensicherung (Backup) ist gewährleistet
- Virenschutz/Firewall nach aktuellem Stand der Technik ist gewährleistet
- Vertretungsregelungen in Bezug auf die Administration kritischer Systeme
- Der Auftragnehmer führt einen Notfallplan zur Dokumentation von Verantwortlichkeiten und Vorgehensweisen im Falle eines Recovery-Falls.

### Availability and Resilience

#### Availability Control

The data center operator is ISO 27001 certified.

A daily disaster recovery backup is created by the hosting subcontractor and stored in a physically separate location.

An additional daily encrypted backup for restoring accidentally deleted partial data is stored for a period of 1 month (s2survey.net) with a separate hosting provider in a separate data center.

#### Hosting and Housing Survey Server (SpaceNet, 2025, p. 14)

- All infrastructure components operated by the Contractor in the SpaceNet data centers are connected to uninterruptible power supply systems and to an emergency power generator (diesel generator).
- The Contractor's data is backed up to a remote data center operated by the Contractor.
- All infrastructure components operated by the Contractor in the SpaceNet data centers are connected to uninterruptible power supply systems and to an emergency power generator (diesel generator).
- The Contractor's data is backed up to a remote data center operated by the Contractor.
- Ensuring that systems can be restored in the event of a failure.
- A regular backup procedure is in place
- Separate storage of production data and backup data is ensured
- State-of-the-art virus protection and firewall are in place
- Procedures for designating alternates for the administration of critical systems
- The contractor maintains an emergency plan to document responsibilities and procedures in the event of a recovery scenario.
- The recovery plan is reviewed at least once a year and updated as necessary.

- Der Recovery-Plan wird mindestens einmal pro Jahr überprüft und ggf. angepasst.

#### **Hosting und Housing Datensicherung (Hetzner, 2026, S. 10-14)**

- 24/7 technischer Support direkt im Rechenzentrum
- Monitoring
- Unterbrechungsfreie Stromversorgung durch redundante USVs und NEA
- Redundante Stromeinspeisung vom Umspannwerk
- Redundante und energieeffiziente Kühlung durch direkte freie Kühlung und Klimaanlage
- Kaltgangeinhausung in überdurchschnittlich hohem Doppelboden
- Überwachung der prozessrelevanten Größen über intelligentes Mess-, Steuer-, Regel- und Überwachungssystem
- Flächendeckende Brandfrüherkennungsmechanismen mit automatischer Alarmierung und Leitstellenanbindung
- Dynamisches Brandschutzkonzept
- Regelmäßige Schulungen und Notfallübungen der Brandschutzhelfer
- Redundante und hochverfügbare Netzwerkinfrastruktur
- Dauerhaft aktive DDoS-Erkennung

#### **Hosting und Housing Backup (Hetzner, 2026, p. 10-14)**

- 24/7 technical support directly at the data center
- Monitoring
- Uninterruptible power supply via redundant UPS systems and NEA
- Redundant power supply from the substation
- Redundant and energy-efficient cooling via direct free cooling and air conditioning systems
- Cold aisle containment in an above-average raised floor
- Monitoring of process-relevant parameters via an intelligent measurement, control, regulation, and monitoring system
- Comprehensive early fire detection systems with automatic alerts and connection to control centers
- Dynamic fire safety plan
- Regular training and emergency drills for fire safety officers
- Redundant and highly available network infrastructure
- Continuous DDoS detection

## **4. Regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit des internen Datenschutzes**

### **4.1. Incident Response Management**

Der technische Betrieb der Befragungsserver ist an einen Subunternehmer (Hoster) ausgelagert. Zum Havarie-Konzept und Notfallplan für IT-Ausfall wird auf dessen TOM verwiesen (SpaceNet, 2025, S. 15):

- Brute-force Schutz vor Angriffen auf Nutzerzugänge.
- Virenschutz ist auf allen Desktop- und Laptop-Rechnern im Netzwerk des Webhoster vorgeschrieben. Es werden auf Netzwerkebene Angriffserkennungssysteme (IDS) eingesetzt, um eine Warnung vor etwaigen Angriffen zu erhalten.
- Der Webhoster führt einen Incident Management

## **Regular Review, Assessment and Evaluation of the Effectiveness of Internal Data Protection**

### **Incident Response Management**

The technical operation of the survey servers is outsourced to a subcontractor (hoster). For the emergency concept and contingency plan for IT failure, reference is made to its TOM (SpaceNet, 2025, p. 15).

- Brute-force protection against attacks on user accounts.
- Antivirus software is required on all desktop and laptop computers within the web host's network. Intrusion detection systems (IDS) are deployed at the network level to provide alerts in the event of attacks.
- The web host maintains an Incident Management

Plan zur Dokumentation von Verantwortlichkeiten und Vorgehensweisen im Falle eines Incidents.

- Auswertung von Meldungen und Berichten zu ungewöhnlichen Vorkommnissen
- Untersuchung erkannter oder vermuteter Verstöße gegen sicherheitsrelevante Vorgaben
- Der Incident Management Plan wird in regelmäßigen Abständen auf seine Umsetzung und Wirksamkeit im Rahmen von internen Audits geprüft und ggf. angepasst.

#### 4.2. Auftragskontrolle

Im Regelfall werden die personenbezogenen Daten automatisiert durch die Befragungssoftware erhoben, verarbeitet, gespeichert und an den Verantwortlichen übermittelt. Diese Funktionen werden über die Benutzeroberfläche bereitgestellt.

Im Regelfall erfolgt durch den Auftragnehmer keinerlei manuelle Verarbeitung der personenbezogenen Daten, die im Auftrag verarbeitet werden, außer es liegt eine schriftliche Weisung des Auftraggebers vor.

Weitere Auftragnehmer (Subunternehmer) werden durch die Geschäftsführung ausgewählt.

Die Aufteilung der Rechte und Pflichten zwischen Auftragnehmer und Auftraggeber geschieht über einen Auftragsverarbeitungsvertrag nach Artikel 28 DSGVO.

#### 4.3. Datenschutzmanagement

Die Planung des Datenschutzmanagements erfolgt gemeinsam mit einem externen Datenschutzbeauftragten unter Einbindung der Geschäftsführung. Dabei werden Datenschutzziele definiert und der Handlungsbedarf ermittelt und priorisiert.

Plan to document responsibilities and procedures in the event of an incident.

- Evaluation of notifications and reports regarding unusual occurrences.
- Investigation of identified or suspected violations of security-related requirements
- The Incident Management Plan is reviewed at regular intervals to assess its implementation and effectiveness as part of internal audits and is adjusted as necessary.

#### Order Control

Generally, personal data is automatically collected, processed, stored and transmitted to the controller by the survey software. These functions are accessed via the user interface.

Generally, there is no manual processing of the personal data that is processed on behalf of the controller, unless there is a written instruction from the controller.

Contractors (subcontractors) are selected by the management.

The division of rights and obligations between the contractor and the client is carried out by means of an data processing agreement (DPA) in accordance with Article 28 GDPR.

#### Data Protection Management

Data protection management is planned together with an external data protection officer with the involvement of the management. Data protection goals are defined and the need for action is determined and prioritized.