

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

zwischen

Beispiel GmbH
Musterstraße 47
12345 Musterstadt

**Muster – korrekte
Daten eingeben unter
s2survey.net/DSGVO/**

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

und

SoSci Survey GmbH
Erchanbertstr. 6
81929 München

vertreten durch die Geschäftsführer Dr. Dominik Leiner und Stefanie Leiner

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

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

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 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 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.
- 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.

2. Bestimmung des Auftragsgegenstandes, Laufzeit

- 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, ins-

besondere 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. **Muster – Daten eingeben unter s2survey.net/DSGVO/**
- 2.4. Die Laufzeit dieser Vereinbarung ist befristet bis zum **31.10.2022**. Der Vertrag beginnt mit der Unterzeichnung der vorliegenden Vereinbarung, nicht jedoch vor Wirksamkeit der zugrunde liegenden Hauptleistungsvereinbarung. 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 Nutzungsvereinbarungen 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) ist vorab die schriftliche Zustimmung des Auftraggebers einzuholen. Der Auftragnehmer hat auf Anforderung des Auftraggebers an der Erstellung der Verarbeitungsverzeichnisse 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:

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

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 des Auftraggebers 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

gen 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 erlaubt 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

Anschrift wie Auftraggeber

Clemens Druckmann

Telefon: +49 (89) 1234- 9876

E-Mail: c.druckmann@example.com

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 Einzelfall 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

**Muster – korrekte
Daten eingeben unter
s2survey.net/DSGVO/**

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 Auftraggeber 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 3 genannten Rechte der betroffenen Person, ebenso bei Datenschutz-Folgeabschätzungen und vorherigen Konsultationen. Zudem hat er Meldepflichten bei Datenpannen. 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 Sicherheitslücken 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 Zu-

sammenhang 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 Auskunftersuchens, 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.

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.
- 9.5. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, insbesondere aus Aufbewahrungsverpflichtungen aus Unionsrecht oder dem für den Auftragnehmer geltenden 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:
- PartnerGate GmbH (VPS-Hosting Webserver)
Wilhelm-Wagenfeld-Str. 16
80807 München
 - 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 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 sechs 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 sechs 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 EU/dem 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 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 der DSGVO 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 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 verhältnismäßige 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 **120 € 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 Formklausel. Dokumentierte Form im Sinne dieses Vertrages meint mindestens die Textform. Auf Verlangen einer Partei ist eine in Textform abgegebene Erklärung schriftlich zu bestätigen.

Für den Auftraggeber

Für den Auftragnehmer

Ort, Datum

München, den 24. Sep. 2024

Name und Position in Blockschrift

Dr. Dominik Leiner, Geschäftsführer

Unterschrift, ggf. Stempel

Unterschrift

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)

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

2. Kategorien von der Verarbeitung betroffener Personen

- Mitarbeiter des Auftraggebers
- 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

**Muster – korrekte
Daten (u.a.
Kategorien von
Betroffenen und
verarbeiteten Daten)
eingeben unter
s2survey.net/DSGVO/**

- 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 originäre 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.

4. Dauer der Datenverarbeitung

Die Dauer der Bearbeitung wurde in der jeweiligen Nutzungsvereinbarung vereinbart.

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.

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 TTDSG sowie die Verletzung der 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., TTDSG, 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.

München, den 24. Sep. 2024

Dr. Dominik Leiner

(für sich persönlich wie in seiner Funktion als Geschäftsführer für die Gesellschaft handelnd)

Anlage 3

Technische und organisatorische Maßnahmen des Auftragnehmers (TOM)

Stand vom 18.11.2024

Rahmeninformation

Als organisatorischer Hintergrund zu den technischen und organisatorischen Maßnahmen der SoSci Survey GmbH (Verarbeiter) seien die folgenden Informationen vorangestellt:

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) greift der Webhoster auf die Leistungen eines weiteren Unternehmens (Betreiber des Rechenzentrums) zurück, welches allerdings kein Subunternehmer im Sinne der DSGVO ist.

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 Rechenzentrums, welche dem Verarbeiter vorliegen und auf Anfrage eingesehen werden können.

- Bei Nutzung des Befragungsservers **s2survey.net** findet im Regelfall keine Verarbeitung auf den Anlagen des Verarbeiters 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 Verarbeiters 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.

1. Vertraulichkeit

1.1. Zutrittskontrolle

Befragungsserver

Hinsichtlich der Serverräume wird auf die technische und organisatorische Maßnahmen (TOM) des Webhosters (nachfolgend zitiert) und des Rechenzentrums verwiesen:

Alle Datenräume sind als separate IT Sicherheitsräume im Sinne des IT- Grundschieutskataloges, herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik (BSI), gemäß Anforderung der Kategorie "Grundschieut" ausgerüstet.

Die Datensicherheitsräume bieten Schutz vor folgenden Risiken:

- Feuer nach DIN 4102-2 / F90, mit bauaufsichtlicher Zulassung
- Temperaturgrenzwerte und Luftfeuchte für 30 Minuten gem. EN 1047-2
- Rauehschutz nach DIN 18095
- unbefugter Zutritt / Einbruchhemmung WK II nach EN 1627
- Lösehwassereintritt mit Wasserdiehtigkeitsnachweis gem. EN 60529 / IP 56
- Staubdichtigkeit gemäß EN 60529
- Schutz gegen Sabotage / Vandalismus
- EMV-Schutz
- Schutz gegen erhöhte Trümmerlasten

1.2. Zugangskontrolle

Sämtliche Datenverarbeitungssysteme (sowohl lokal wie auch die eingesetzten Befragungsserver) sind mittels Passwörtern gesichert. Dabei werden mindestens die folgenden Standards eingehalten:

Mindeststandards für Passwörter	<ul style="list-style-type: none">• Unterschiedliche Zeichenzusammensetzung• Mindestlänge 16 Zeichen• Zugangssperre bei mehr als 3 Anmeldeversuchen
Verwaltung der Passwörter	<ul style="list-style-type: none">• Etablierte Open Source Software• Schutz des Zugriffs durch 2-Faktor Authentifizierung

Befragungsserver

Auf Software und Konfiguration basierende Zugangskontrollen:

Verwendete Server-Software	<ul style="list-style-type: none">• Gängige Linux-Distribution (Open Source)• Gängige Webserver-Anwendungen (Open Source)
Beschränkung von Server-Zugriffen	<ul style="list-style-type: none">• Beschränkung auf notwendige Ports (HTTP, HTTPS, E-Mail) mittels interner Firewall (iptables)• Die Fernwartung ist nur für ausgewählte IP-Adressen erreichbar.
Sicherheitsupdates	<ul style="list-style-type: none">• Sicherheitsupdates werden automatisiert mehrmals täglich installiert.
Verschlüsselung	<ul style="list-style-type: none">• Die Daten werden verschlüsselt gespeichert (data at rest encryption), ausgenommen sind Datei-Uploads der Befragten im Fragebogen.

Hinsichtlich der physischen Zutrittskontrollen zum Webserver wird erneut auf die TOM des Webhosters verwiesen, nachfolgend zitiert:

Nur befugte Personen haben Zugang zu den DV-Anlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden.

Festlegung befugter Personen	<ul style="list-style-type: none"> • Räume sind verschlossen und nur befugte Personen haben einen Schlüssel • Zutrittsüberwachung im RZ • Biometrische Sicherheitssysteme für die Büro- und RZ-Flächen • Chipkarten-/Transponder für Sicherheitsbereiche
Regelungen für Firmenfremde	<ul style="list-style-type: none"> • Betriebsfremde Personen haben keinen Zugang zu den DV-Anlagen
Sicherung außerhalb der Arbeitszeit	<ul style="list-style-type: none"> • Alle Räume sind verschlossen • Kameraüberwachung
Workstations und Notebooks	<ul style="list-style-type: none"> • Notebooks sind verschlüsselt • Authentifizierung über Benutzername/Passwort • Interne Sicherheitsrichtlinie für den Umgang mit DV-Systemen
Verpflichtung auf das Datengeheimnis	<ul style="list-style-type: none"> • Wird bei jedem Mitarbeiter durchgeführt
Benutzerberechtigungen	<ul style="list-style-type: none"> • Werden durch den Leiter IT vergeben
Einsatz von 2-Factor	<ul style="list-style-type: none"> • Wo es möglich ist, wird eine 2-Factor Authentifizierung verwendet
Vernichtung von Datenträgern	<ul style="list-style-type: none"> • Wird durch ein zertifiziertes Unternehmen durchgeführt • Die Vernichtung wird protokolliert
Remotezugriff	<ul style="list-style-type: none"> • Der administrative Remotezugriff auf die DV-Anlagen ist ausschließlich über ein VPN möglich
IT-Sicherheit	<ul style="list-style-type: none"> • Einsatz diverser Antivirenlösungen • Einsatz von Hard- und Softwarefirewalls

Verwaltungssysteme

Personenbezogene Daten werden im Regelfall nicht auf den Verwaltungssystemen oder externen/mobilen Medien gespeichert. Sollte dies im Ausnahmefall 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.

1.3. Zugriffskontrolle

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

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

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).

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.

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

2.Integrität

2.1. Weitergabekontrolle

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.

Hardware-basierte Maßnahmen

Für den Maßnahmen zur physischen Weitergabekontrolle wird auf die TOM des Webhosters verwiesen, nachfolgend zitiert:

Festlegung befugter Personen	<ul style="list-style-type: none">Durch die Vergabe entsprechender Rechte
Datenträger	<ul style="list-style-type: none">Mobile Datenträger werden in der Regel nicht verwendet. Speicherung findet auf fest montierten Festplatten stattFestplatten werden überwacht und werden in den Server-Racks verschlossen
Auswahl der Auftragnehmer	<ul style="list-style-type: none">Auswahl erfolgt in der Regel durch Leiter IT oder GF
Aufteilung der Rechte und Pflichten zw. Auftragnehmer und Auftraggeber	<ul style="list-style-type: none">Geschieht über einen AV-Vertrag nach Artikel 28 DSGVO
Kontrolle der Auftragnehmer	<ul style="list-style-type: none">Geschieht durch den Leiter IT und den Datenschutzbeauftragten

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.

3. Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle

Die Dienstleistungen werden mit Hilfe eines Rechenzentrumsdienstleisters erbracht, welcher nach ISO 27001 zertifiziert ist. Für detaillierte Informationen wird auf die TOM der *m-net GmbH* verwiesen.

Ein Disaster Recovery Backup wird durch den Hosting Subunternehmer erstellt und physikalisch und örtlich getrennt aufbewahrt.

Ein zusätzliches tägliches, verschlüsseltes Backup zur Wiederherstellung versehentlich gelöschter Teildaten wird für den Zeitraum von 1 Monat (s2survey.net) auf einem getrennten System im gleichen Rechenzentrum gespeichert und automatisiert gelöscht.

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.

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 AV-Vertrag 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.

Muster - nicht manuell ändern