Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DS-GVO zwischen

dem Kunden
als Verantwortlicher (hier bezeichnet als „Auftraggeber“)

und

GESIS – Leibniz-Institut für Sozialwissenschaften e.V., B6 4-5, 68159 Mannheim,
als Auftragsverarbeiterin (hier bezeichnet als „Auftragnehmer“)

Präambel

Der Auftraggeber möchte den Auftragnehmer mit den in § 3 genannten Leistungen beauftragen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DS-GVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung, deren Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

§ 1 Begriffsbestimmungen

In diesem Vertrag verwendete Begriffe, die in Art. 4, 9 und 10 DS-GVO definiert werden, sind im Sinne dieser gesetzlichen Definition zu verstehen.

§ 2 Vertragsgegenstand

(1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich der Gebrauchsüberlassung von Software auf Grundlage des zwischen dem Auftraggeber und dem Auftragnehmer geschlossenen Vertrags („Hauptvertrag“). Der Hauptvertrag kam durch Zustimmung des Auftraggebers zu den Nutzungsbedingungen für die Nutzung der Software GESIS AppKit („Software“) zustande.

Der Auftragnehmer erhält Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers, sofern der Auftragnehmer nicht durch das Recht der Union oder der Mitgliedsstaaten, dem er unterliegt, zu einer anderen Verarbeitung verpflichtet ist. Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus dem Hauptvertrag (und sofern vorhanden aus der dazugehörigen Leistungsbeschreibung) sowie aus der **Anlage 1** zu diesem Vertrag. Dem Auftraggeber obliegt die alleinige Beurteilung der Zulässigkeit der Datenverarbeitung gemäß Art. 6 Abs. 1 DS-GVO. Der Auftraggeber bleibt jederzeit für die Einhaltung seiner Verpflichtungen als Verantwortlicher für die Verarbeitung nach diesem Auftragsverarbeitungsvertrags verantwortlich. Der Auftraggeber wird insbesondere

(a) sicherstellen, dass die Informationen in Anlage 1 “Beschreibung der betroffenen Personen/Betroffenengruppen sowie der besonders schutzbedürftigen Daten/Datenkategorien” richtig und vollständig sind. Hierzu kann sich der Auftraggeber jederzeit Kontakt mit dem Auftragnehmer unter appkit@gesis.org aufnehmen.

(b) den betroffenen Personen alle nach den gesetzlichen Bestimmungen über den Datenschutz erforderlichen Informationen und Mitteilungen rechtzeitig zur Verfügung stellen.
(c) sicherstellen, dass er gegenüber den betroffenen Personen jederzeit über eine gesetzliche Grundlage nach den gesetzlichen Bestimmungen über den Datenschutz für die Verarbeitung aller personenbezogenen Daten verfügt und aufrechterhält, die er durch die Nutzung der Software verarbeitet /einschließlich der Einholung wirksamer, informierter Einwilligungen von betroffenen Personen).
(d) den Auftragnehmer unverzüglich informieren, falls i) die Rechtsgrundlage für die Datenverarbeitung des Auftraggebers gemäß den gesetzlichen Bestimmungen über den Datenschutz wegfällt (z.B. Widerruf der Einwilligung durch die betroffene Person) und ii) der Auftraggeber Informationen erlangt, die den Verdacht eines unbefugten Zugriffs oder einer unbefugten Verarbeitung personenbezogener Daten begründen. Der Auftraggeber hat dem Auftragnehmer alle relevanten Informationen zur Verfügung zu stellen.

(2) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

(3) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden oder auf sonstige Weise in dessen Auftrag verarbeitet werden.

(4) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

(5) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der europäischen Union oder einem anderen Vertragsstaat des Abkommens über den europäischen Vertragsraum (Beschluss 94/1/EG) statt. Jede Verlagerung von Teilleistungen oder der gesamten Dienstleistung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers in Schriftform oder dokumentiertem elektronischen Format und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

§ 3 Art der verarbeiteten Daten, Kreis der betroffenen Personen

Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragnehmer Zugriff auf die in **Anlage 1** näher spezifizierten personenbezogenen Daten der ebenfalls in **Anlage 1** näher spezifizierten betroffenen Personen. Diese Daten umfassen die in **Anlage 1** aufgeführten und als solche gekennzeichneten besonderen Kategorien personenbezogener Daten.

§ 4 Weisungsrecht

(1) Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers erheben, nutzen oder auf sonstige Weise verarbeiten; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

(2) Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in dokumentiertem elektronischen Format durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten. Die weisungsberechtigten Personen ergeben sich aus **Anlage 4**. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen ist dem Vertragspartner unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen.

(3) Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren und für die Dauer ihrer Geltung sowie anschließend für drei weitere volle Kalenderjahre aufzubewahren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers an den Auftragnehmer entstehen, bleiben unberührt.

(4) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 5 Schutzmaßnahmen des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird und gewährleistet, dass er alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DS-GVO, insbesondere mindestens die in **Anlage 2** aufgeführten Maßnahmen getroffen hat. Sofern auch besondere Kategorien personenbezogener Daten verarbeitet werden, trifft der Auftragnehmer zusätzlich die sich aus § 22 Absatz 2 BDSG ergebenden angemessenen und spezifischen Maßnahmen. Der Auftragnehmer legt auf Anforderung des Auftraggebers die näheren Umstände der Festlegung und Umsetzung der Maßnahmen offen.

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Beim Auftragnehmer ist als betrieblicher Datenschutzbeauftragter bestellt:

HEC Harald Eul Consulting GmbH
Datenschutzbeauftragte GESIS
Auf der Höhe 34
50321 Brühl
E-Mail: Datenschutz-GESIS@he-c.de
Telefon: +49 (0) 2232/200 879

(4) Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu nutzen oder auf sonstige Weise zu verarbeiten. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im Folgenden Beschäftigte genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DS-GVO) und über die sich aus diesem Vertrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehren sowie mit der gebotenen Sorgfalt die Einhaltung der vorgenannten Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Beschäftigten und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

(5) Die Verarbeitung von Daten, die Gegenstand dieses Vertrags sind, in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) ist nur mit Zustimmung des Auftraggebers gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicherzustellen. Die Einhaltung der Schutzmaßnahmen nach § 6 Absätzen 1 und 2 dieses Vertrags sowie der Maßgaben des Art. 32 DS-GVO ist auch in diesem Fall sicherzustellen.

§ 6 Informationspflichten des Auftragnehmers

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder dokumentiertem elektronischen Format informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält soweit möglich folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;

b) eine Beschreibung der wahrscheinlichen Folgen der Verletzung und

c) eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(2) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Person(en), informiert hierüber den Auftraggeber und ersucht diesen um weitere Weisungen.

(3) Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.

(4) Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Pflichten des Auftraggebers nach Art. 33 und 34 DS-GVO in angemessener Weise (Art. 28 Abs. 3 S. 2 lit. f DS-GVO). Meldungen für den Auftraggeber nach Art. 33 oder 34 DS-GVO darf der Auftragnehmer nur nach vorheriger Weisung seitens des Auftraggebers gem. § 5 dieses Vertrags durchführen.

(5) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der DS-GVO liegt.

(6) Über wesentliche Änderungen der Sicherheitsmaßnahmen nach § 6 Abs. 2 dieses Vertrags hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten.

(7) Ein Wechsel in der Person des betrieblichen Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

(8) Der Auftragnehmer und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DS-GVO enthält. Das Verzeichnis ist dem Auftraggeber auf Anforderung zur Verfügung zu stellen.

(9) An der Erstellung des Verfahrensverzeichnisses durch den Auftraggeber sowie bei der Erstellung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO und ggf. bei der vorherigen Konsultation der Aufsichtsbehörden gemäß Art. 36 DS-GVO hat der Auftragnehmer im angemessenen Umfang mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

§ 7 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers. Hierfür kann er z. B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche, schriftliche oder elektronische Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind.

(3) Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

(4) Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung.

(5) Der Auftragnehmer weist dem Auftraggeber die Verpflichtung der Mitarbeiter nach § 6 Abs. 4 auf Verlangen nach.

(6) Der Auftraggeber vergütet dem Auftragnehmer den Aufwand, der ihm im Rahmen der Kontrolle entsteht.

§ 8 Einsatz von Subunternehmern

(1) Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen nicht zur Begründung von Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt.

(2) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

§ 9 Anfragen und Rechte betroffener Personen

(1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32 und 36 DSGVO.

(2) Macht eine betroffene Person Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist die betroffene Person unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

(3) Der Auftragnehmer gewährt dem Auftraggeber gemäß der in dem Hauptvertrag getroffenen Übereinkunft jederzeit den elektronischen Zugang zu einer Internet-basierten Software-Plattform, in der die personenbezogenen Daten der betroffenen Personen gespeichert sind, so dass der Auftraggeber auf eigenen Wunsch jederzeit personenbezogene Daten löschen, freigeben, korrigieren, exportieren, speichern oder den Zugriff hierauf sperren kann.

(4) Der Auftraggeber kann den Auftragnehmer, soweit gesetzlich zulässig, detaillierte schriftliche Anweisungen zur Löschung, Freigabe, Berichtigung, zum Export, zur Speicherung oder zur Sperrung personenbezogener Daten der betroffenen Person erteilen. Verlangt der Auftraggeber, dass der Auftragnehmer eine solche Löschung, Freigabe, Berichtigung, Export, Speicherung oder Sperrung von Daten vornimmt, die der Auftraggeber hätte vornehmen können, so kann der Auftragnehmer eine für eine solche Leistung angemessene Vergütung verlangen.

(5) Sofern der Auftraggeber infolge der Nutzung der Software keine Möglichkeit hat, personenbezogene Daten gemäß den gesetzlichen Bestimmungen über den Datenschutz zu korrigieren, zu ändern, zu sperren oder zu löschen, wird der Auftragnehmer auf Wunsch des Auftraggebers alles Notwendige unternehmen, um solche Handlungen zu ermöglichen, soweit dies dem Auftragnehmer rechtlich gestattet ist.

(6) Der Auftraggeber weist den Auftragnehmer an, im Rahmen des technisch Möglichen den Zugang zu den personenbezogenen Daten der betroffenen Personen und die Möglichkeit, diese zu bearbeiten, zu verschaffen.

(7) Die rechtliche Verantwortung dafür, dass die Datenverarbeitung mit den geltenden gesetzlichen Bestimmungen über den Datenschutz vereinbar ist, wenn der Auftraggeber auf die personenbezogenen Daten einzelner betroffener Personen zugreift und diese bearbeitet, liegt ausschließlich beim Auftraggeber.

(8) Der Auftragnehmer wird den Auftraggeber bei der Bearbeitung von Anfragen betroffener Personen auf Zugang zu ihren personenbezogenen Daten in angemessener Weise unterstützen und dem Auftraggeber behilflich sein, soweit dies gesetzlich zulässig ist und soweit der Auftraggeber keine Möglichkeit besitzt, die Ansprüche der betroffenen Personen durch die Nutzung der Software oder der Services selbst zu erfüllen.

§ 10 Haftung

(1) Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung. Der Auftragnehmer stimmt eine etwaige Erfüllung von Haftungsansprüchen mit dem Auftraggeber ab.

(2) Der Auftragnehmer stellt den Auftraggeber auf erstes Anfordern von sämtlichen Ansprüchen frei, die betroffene Personen gegen den Auftraggeber wegen der Verletzung einer dem Auftragnehmer durch die DSGVO auferlegten Pflicht oder der Nichtbeachtung oder Verletzung einer vom Auftraggeber in dieser AV-Vereinbarung oder einer gesondert erteilten Anweisung geltend machen.

(3) Die Parteien stellen sich jeweils von der Haftung frei, wenn / soweit eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einer betroffenen Person eingetreten ist, verantwortlich ist. Im Übrigen gilt Art. 82 Absatz 5 DS-GVO.

(4) Sofern vorstehend nicht anders geregelt, entspricht die Haftung im Rahmen dieses Vertrages der des Hauptvertrages.

§ 11 Außerordentliches Kündigungsrecht

Der Auftraggeber kann den Hauptvertrag fristlos ganz oder teilweise kündigen, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DS-GVO oder sonstige anwendbare Datenschutzvorschriften vorsätzlich oder grob fahrlässig verletzt oder eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer sich den Kontrollrechten des Auftraggebers auf vertragswidrige Weise widersetzt. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

§ 12 Beendigung des Hauptvertrags

(1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen.

(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht.

(3) Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

§ 13 Schlussbestimmungen

(1) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Die Ersetzung der Schriftform durch die elektronische Form (§§ 126 Abs. 3, 126a BGB) oder die Textform (§ 126b BGB) ist ausgeschlossen.

Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

(3) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

(4) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Mannheim.

<u>Anlagen:</u>

Anlage 1 – Beschreibung der betroffenen Personen/Betroffenengruppen sowie der besonders schutzbedürftigen Daten/Datenkategorien

Anlage 2 – Technische und organisatorische Maßnahmen des Auftragnehmers

Anlage 3 – Genehmigte Subunternehmer

Anlage 4 – Weisungsberechtigte Personen

Anlage 1 – Beschreibung der betroffenen Personen/Betroffenengruppen sowie der besonders schutzbedürftigen Daten/Datenkategorien

Als Verantwortlicher legt der Auftraggeber die Kategorien betroffener Personen fest. Sofern der Auftraggeber keine Kategorien von betroffenen Personen spezifiziert hat, werden die Daten der Nutzer der Software (Studienteilnehmende), die vom Auftraggeber eingeladen werden, an Studien teilzunehmen und Informationen mitzuteilen, verarbeitet.

In seiner Rolle als Verantwortlicher für die Verarbeitung wird der Auftraggeber die Arten personenbezogener Daten spezifizieren. Sofern der Auftraggeber keine Arten personenbezogener Daten spezifiziert hat, können aufgrund der Nutzung der Software folgende Arten personenbezogener Daten der Nutzer der Software verarbeitet werden: Nutzer-ID, Datum und Uhrzeit der Nutzung der Software, Gerätehersteller, Betriebssystem sowie alle durch den Auftraggeber abgefragten Studiendaten (z.B. Alter; Geschlecht; Familienstand; Anzahl der Kinder; Interessengebiete; personenbezogene Daten, die die Nutzer beispielsweise in offenen Textfeldern mitteilen; durch die Nutzer der Software aufgenommenen Bilder/Bilddaten).

Als Verantwortlicher kann der Auftraggeber entscheiden, ob er besondere Kategorien personenbezogener Daten im Sinne von Artikel 9, 10 DSGVO erheben und verarbeiten möchte. Zu den besonderen Kategorien personenbezogener Daten zählen Daten,

- aus denen die rassische und ethnische Herkunft,
- politische Meinungen,
- religiöse oder weltanschauliche Überzeugungen oder
- die Gewerkschaftszugehörigkeit hervorgehen, sowie
- die Verarbeitung von genetischen Daten,
- biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person,
- Gesundheitsdaten
- Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person oder
- die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten

Technische und organisatorische Maßnahmen nach Art. 32 Abs. 1 DSGVO

von

GESIS – Leibniz-Institut für Sozialwissenschaften e.V.

Version: 2.0

Fassung vom: 03.04.2024

Einführung

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen, werden die nachfolgenden technischen und organisatorischen Maßnahmen (TOM) festgelegt.

Bei der Auswahl der Maßnahmen wurden die vier Schutzziele des Art. 32 Abs. 1 b) DSGVO, namentlich die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme, berücksichtigt. Eine rasche Wiederherstellung nach einem physischen oder technischen Zwischenfall ist gewährleistet. Alle technischen und organisatorischen Maßnahmen werden regelmäßig gemäß Art. 32 Abs. 1 d) DSGVO auf ihre Wirksamkeit hin geprüft.

Vertraulichkeit

Zutrittskontrolle

Bei der Zutrittskontrolle handelt es sich um Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Es wird zwischen dem Zutritt zu den Büroflächen und den Rechenzentren des Instituts unterschieden.

Grundsätzliche Maßnahmen zur Zutrittskontrolle bei GESIS

In den Büroflächen des Instituts werden IT-Systeme betrieben, die für die Administration der technischen Systeme erforderlich sind. Zutritt zu diesen Räumlichkeiten haben nur berechtigte Mitarbeitende. Für die physische Absicherung der Büroräume sind unter anderem folgende Maßnahmen ergriffen worden:

- Verwendung von Sicherheitstüren und -schlössern zum Schutz des Gebäudes
- Zutrittskontrollsystem
- Manuelles und/oder Transponder-Schließsystem an den Büros der IT
- Manuelles Schließsystem an den Büros der Personalabteilung
- Anmelde- und Aufenthaltsregelungen für betriebsfremde Personen
- Besetzter Empfang
- Personenkontrolle beim Empfang mit Besucherbuch
- Bestreifung des Gebäudes in Mannheim durch einen Wachdienst außerhalb der Dienstzeit
- Betrieb einer Alarmanlage für das Rechenzentrum in Köln

Grundsätzliche Maßnahmen zur Zutrittskontrolle in Rechenzentren

Die Hardware für die zentralen Server- und Storage-Systeme der GESIS befindet sich in den Rechenzentren der GESIS in Köln und Mannheim.

Die Rechenzentren sind als zutrittsbeschränkte Sicherheitsbereiche ausgelegt. Eine effektive Zutrittskontrolle wird durch die Kombination von verschiedenen, ineinandergreifenden Maßnahmen umgesetzt. Hierzu zählen unter anderem folgende technische und organisatorische Maßnahmen:

- Verwendung von Sicherheitstüren und -schlössern
- Manuelles und Transponder-Schließsystem
- Einsatz von Gefahrenmeldeanlagen (Einbruchmelder, Bewegungsmelder, Türkontakte) in Köln
- Regelungen zur Verwaltung und Dokumentation von Zutrittsberechtigungen
- Verbindliche Verfahren zur Einrichtung, Änderung und dem Entzug von Zutrittsberechtigungen

- Nur die IT-Mitarbeitenden der Standorte Köln und Mannheim sowie angemeldete Mitarbeitende definierter Dienstleister haben eine Zutrittsberechtigung. Der Zutritt zu den Sicherheitsbereichen wird betriebsfremden Personen, auch Mitarbeitenden der GESIS, erst nach Anmeldung und nur in Begleitung eines zutrittsberechtigten Mitarbeitenden des Rechenzentrums ermöglicht.

Zugangskontrolle

Bei der Zugangskontrolle handelt es sich um Maßnahmen, die geeignet sind, das technische Eindringen Unbefugter in die Datenverarbeitungsanlagen zu verhindern. Insbesondere durch Benutzeridentifikation und Authentifizierung.

Grundlegende Maßnahmen

Im Umfeld der Zugangskontrolle sind unter anderem folgende grundlegende Maßnahmen umgesetzt:

- verbindliche Verfahren zur Einrichtung von Benutzerkonten und Gruppen
- verbindliche Nutzung von sicheren Passwörtern entsprechend der Passwortrichtlinie (Zeichen-Mix („3 von 4“), mind. 8 Zeichen, regelmäßiger Wechsel alle 180 Tage, Passworthistorie)
- revisionssicheres, verbindliches Verfahren zur Rücksetzung „vergessener“ Passwörter
- Authentifikation mit Benutzername und Passwort zwingend
- Temporäre Unmöglichkeit der Authentifikation bei mehrfach fehlerhafter Eingabe des Passworts
- Einsatz von kryptographischen Mechanismen in Übertragungsprotokollen, bei der Authentifizierung und Verschlüsselung entsprechend dem Stand der Technik
- Regelungen für die mobile Nutzung des VPN-Zugangs durch Mitarbeitende
  - Eine VPN-Einwahl erfolgt ausschließlich unter Nutzung von verschlüsselten Verbindungen, es bestehen strikte Firewall-Regeln gemäß Erforderlichkeit zur Aufgabenerfüllung und nach dem Stand der Technik
- Die Computer der Mitarbeitenden und die Server verfügen über Virenscanner
- Die Computer der Mitarbeitenden arbeiten mit einer Festplattenverschlüsselung
- Eine automatische Sperrung des Logins an den Arbeitsplatzrechner tritt nach 10 Minuten in Kraft. Die Mitarbeitenden sind angehalten diese beim Verlassen des Arbeitsplatzes zu aktivieren oder sich abzumelden. Eine Aufhebung der Sperre erfolgt nur durch Eingabe eines Passworts.
- Einsatz von Hardware- und Software-Firewalls und Protokollierung relevanter Systemmeldungen und Alarmierung bei ungewollten Vorfällen
- Die Benutzer-Accounts ausgeschiedener Mitarbeiter werden am letzten Arbeitstag deaktiviert
- Protokollierung der Anmeldung auf Betriebssystemebene ist möglich

Zugangskontrolle zu IT-Systemen

Der Zugang zu allen IT-Systemen ist nur nach Eingabe von Benutzerkennung und Passwort entsprechend der Passwortrichtlinie möglich. Der Fernzugriff auf IT-Systeme erfolgt ausschließlich unter Verwendung von verschlüsselten Administrationsprotokollen. Die Netzbereiche sind entsprechend eines Zonenkonzepts segmentiert und die Netzübergänge werden durch Firewalls geschützt. Es werden nur die für die legitime Nutzung des Dienstes notwendige Kommunikation und die erforderlichen Zugänge zur Administration zugelassen.

Zugriffskontrolle

Bei der Zugriffskontrolle handelt es sich um Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die gemäß ihrer Zugriffsberechtigung zugehörenden Daten zugreifen können, und das personenbezogene Daten bei der Verarbeitung,

Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Umsetzung einer nachhaltigen Zugriffskontrolle stellt einen wichtigen Beitrag zur Gewährleistung von Vertraulichkeit und Integrität der eingesetzten IT-Systeme und der dort gespeicherten und verarbeiteten Informationen dar. Dies wird erreicht durch:

- strukturierte Regelwerke unter anderem für Umgang mit Passwörtern, VPN-Einwahl, Datensicherung, Netzwerkkomponenten, Firewalls
- Systemhärtung entsprechend den Empfehlungen der Hersteller und der Best Practices verschiedener Organisationen
- etablierte Vorgehensweisen zur Behandlung von Sicherheits- und Datenschutzvorfällen
- strukturierte und nachvollziehbare Durchführung von Inbetriebnahmen, Änderungen und Rückbauten an Hard- und Softwarekomponenten
- zentrale Rollen- und Berechtigungsvergabe gemäß der Erforderlichkeit zur Aufgabenerfüllung
- Trennung von Berechtigungsbewilligung (organisatorisch) durch Fachabteilung (Abteilungs-/Teamleitung) und Berechtigungsvergabe (technisch) durch IT-Abteilung
- Verwaltung der Rechte durch Systemadministratoren
- Authentisierung gegenüber zentralem Verzeichnisdienst, lokalem Betriebssystem, Applikation
- verbindliches Konzept der Laufwerksnutzung und –zuordnung
- physische Löschung von Datenträgern vor Wiederverwendung
- ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- Zu vernichtende Datenträger werden im gesicherten Bereich der Rechenzentren gesammelt. Die Abholung und Vernichtung erfolgen durch zertifizierte Dienstleister.
- Verschlüsselung von Datenträgern
- Verbot der Speicherung von personenbezogenen Daten auf privaten IT-Systemen oder privater Speichermedien

Pseudonymisierung

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

Trennungskontrolle

Es erfolgt eine restriktive Rechtevergabe bei Anwendungen, Diensten und Dateisystemen unter Berücksichtigung des „Need-to-know”-Prinzips. Beschäftigte erhalten damit nur Zugriff auf diejenigen Daten, deren Kenntnis im Rahmen der Ihnen übertragenen Aufgaben notwendig ist.

Sofern möglich, erfolgt der Einsatz einer spezifischen, gegebenenfalls mandantenfähigen Softwarelösung, um eine logische Trennung der Daten und Verarbeitungen für verschiedene Teilnehmer am Dienst beziehungsweise Zweck zu gewährleisten.

Die Entwicklungs- und Testsysteme sind strikt von der Produktionsumgebung getrennt.

Verpflichtung der Mitarbeitenden

Alle mit der Verarbeitung betrauten Mitarbeitenden sind auf das Datengeheimnis verpflichtet.

Integrität

Weitergabekontrolle

Bei der Weitergabekontrolle handelt es sich um Maßnahmen, die gewährleisten, das personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Transport der Datenträger durch geeignete und zuverlässige Personen
- Verschlüsselung von Datenträgern bei Transporten
- Nutzung eines sicheren digitalen browserbasierten Transferdienstes mit Verschlüsselung (Transport), automatischer Löschung nach Ablauf des vorgegebenen Zeitintervalls

Eingabekontrolle

Bei der Eingabekontrolle geht es darum, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Die Nachvollziehbarkeit der Verarbeitung von personenbezogenen Daten basiert auf personenbezogenen Kennungen. Die Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten basiert auf einem Berechtigungskonzept (s.o. Zugangs-/Zugriffskontrolle). Die Anforderungen zur Berechtigungsvergabe werden archiviert.

Auf ausgewählten Systemen werden Aktivitäten in administrativen Rollen protokolliert. Zugriff haben nur berechtigte Mitarbeitende. Protokolldateien werden automatisiert gelöscht.

Verfügbarkeit und Belastbarkeit

Bei der Verfügbarkeitskontrolle dient der Sicherstellung des Schutzes von personenbezogenen Daten gegen zufällige Zerstörung oder Verlust. Die Verfügbarkeit und Belastbarkeit der Dienste werden durch eine Reihe von Maßnahmen gewährleistet. Hierzu zählen:

- zuvor beschriebene Maßnahmen zur Gewährleistung einer sicheren Installation, Konfiguration sowie eines sicheren Betriebs
- eine redundante Auslegung der zentralen IT-Systeme an den zwei Standorten Köln und Mannheim (einschließlich Brandschutz, Klimatisierung, USV, NEA (in Köln))
- verschiedene Maßnahmen zur Vermeidung, Erkennung und Abwehr von Angriffen (Firewall, Virenscanner, SPAM-Filter)
- ein Monitoring der Systemumgebung
- ein Konzept für den Umgang mit Datenschutz- und Sicherheitsvorfällen
- ein Backupkonzept mit täglicher Sicherung im sog. Backup-to Disk-to-Cloud-Verfahren
- zur raschen Wiederherstellbarkeit Ausweichalternativen in ein externes Rechenzentrum
- Regelmäßige Überprüfung des Backupverfahrens
- Erhaltene Datenträger werden mit einem Virenscanner auf schadenstiftende Software überprüft, bevor sie verwendet werden
- Wartungsarbeiten werden i.d.R. frühzeitig angekündigt und nach Möglichkeit in den Randstunden durchgeführt

Überprüfung, Bewertung und Evaluierung

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung sind wie folgt umgesetzt:

- Durchführung von Sensibilisierungsmaßnahmen
- Reporting bzw. Berichterstattung
- Prozess zur Behandlung von Datenschutz- und Sicherheitsvorfällen
- Regelmäßige Überprüfung der technischen und organisatorischen Maßnahmen, basierend auf Änderungen am Schutzbedarf der Systeme und deren Alter
- Bestellung eines externen Datenschutzbeauftragten

Auftragskontrolle

Die Auftragskontrolle stellt sicher, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen von GESIS verarbeitet werden können. Hierzu werden etwa folgende Maßnahmen ergriffen:

- Sorgfältige Auswahl des Auftragsverarbeiters
- Dokumentierte Weisungen an den Auftragsverarbeiter
- Verpflichtung der Mitarbeitenden des Auftragsverarbeiters auf Vertraulichkeit
- Auftragsverarbeiter hat möglichst einen Datenschutzbeauftragten benannt
- Sicherstellung der Vernichtung oder Herausgabe von Daten nach Beendigung des Auftrags
- Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragsverarbeiter
- Festlegung technischer und organisatorischer Maßnahmen durch den Auftragsverarbeiter

Weitere allgemeine Maßnahmen

Löschung

Personenbezogene Logdaten werden gelöscht oder anonymisiert, sofern sie nicht gesetzlich oder vertraglich aufbewahrt werden müssen.

Eine Löschung nicht mehr benötigter personenbeziehbarer Daten erfolgt sobald technisch und organisatorisch möglich.

Festplatten werden durch einen spezialisierten Entsorger fachgerecht und datenschutzkonform entsorgt.

Verzeichnis der Verarbeitungstätigkeiten

Verarbeitungen personenbezogener Daten werden gemäß Art. 30 DSGVO dokumentiert.

Dienstspezifische E-Mail-Adressen

Sofern sinnvoll, werden für die Mitarbeitenden im IT-Betrieb dienstspezifische E-Mail-Adressen benutzt, um eine Trennung von der persönlichen Kommunikation der einzelnen Mitarbeitenden und eine ständige Verfügbarkeit der Informationen zu gewährleisten.

Datenschutzfreundliche Voreinstellungen

Die eingesetzten Systeme und Anwendungen werden, soweit technisch möglich, mit Voreinstellungen versehen, die den Grundsätzen der Datenminimierung und Zweckbindung entsprechen.

Datenminimierung

Es werden grundsätzlich nur personenbezogene Daten erhoben bzw. verarbeitet, die für den jeweiligen Verarbeitungszweck erforderlich sind.

Schulung von Mitarbeitenden

Es werden regelmäßige Schulungen zu IT-Sicherheit und Datenschutz mit allen Mitarbeitenden durchgeführt. Darüber hinaus organisiert GESIS eine abteilungsübergreifende Arbeitsgemeinschaft zu datenschutzrechtlichen Themen.

Anlage 3 – Genehmigte Subunternehmer
Im Sinne von §8 gibt es keine genehmigten Subunternehmer.

Anlage 4 – Weisungsberechtigte Personen und Kommunikationsweg zur Weisung

Weisungsberechtigte Person des Auftraggebers ist: Der Kunde als Verantwortlicher

Weisungsempfänger beim Auftragnehmer sind: Mitarbeitende bei GESIS als Auftragsverarbeiterin sind unter der Kontaktadresse appkit@gesis.org zu erreichen

Für die Weisung zu nutzende Kommunikationskanäle: appkit@gesis.org