Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO

Vereinbarung

zwischen

Landesstelle der Psychologischen Beratungsstellen
Susanne Bakaus
in der Evang. Landeskirche in Württemberg
Augustenstr. 39B
70178 Stuttgart

Verantwortlicher: nachstehend *Auftraggeber* genannt

und

SIT Stricker Informationstechnik
Kirchberg 2
74243 Langenbrettach

Auftragsverarbeiter: nachstehend *Auftragnehmer* genannt

1 Gegenstand und Dauer des Auftrags

1.1 Gegenstand ist die Betreuung des EDV-Netzwerkes des Auftraggebers.

a) Betreut werden
- die „Serverlandschaft“ (meist Hyper-V Host-Server und diverse virtuelle Server)
- Arbeitsplätze
- Peripheriegeräte (Drucker, NAS, Lesegeräte, etc.)
- Infrastruktur (Firewall, Router, Switches, EDV-Kabel, etc.)
- gegebenenfalls die Telefonanlage

b) Die Betreuung findet vor Ort und über Fernwartung statt.

c) Benötigt werden dazu Administrator-Rechte auf allen Servern, Arbeitsplätzen und oben genannten Geräten. Der Administrator hat lesenden und schreibenden Zugriff auf alle Laufwerke auf Dateiebene.

d) Tätigkeiten sind:
- Updates und Patches: regelmäßig bei Betriebssystemen, Standardprogrammen wie Virenschutz, Office, etc., nach Aufforderung auch Anwendungsprogramme wie z.B. Buchhaltung, Warenwirtschaft, Pflegeprogramm, etc.
- Fehleranalyse und -behebung
- Installationen gemäß Beauftragung
- Installation neuer Hardware bei Garantiefällen oder auf Absprache.

1.2 Der Auftrag ist unbefristet erteilt und kann von beiden Parteien zu jedem Zeitpunkt ohne Kündigungsfrist beendet werden.

2 Konkretisierung des Auftragsinhalts

2.1 Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Wartung und Pflege von IT-Systemen und IT-Anwendungen gegenüber dem Auftragnehmer zu erteilen. Weisungen können schriftlich, per Fax, per E-Mail oder mündlich erfolgen. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich schriftlich (in einer der genannten Formen).

2.2 Der Auftraggeber ist verantwortliche Stelle i. S. d. Art. 4 Nr. 7 DSVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer und für die die Wahrung der Rechte der betroffenen Personen allein verantwortlich.

2.3 Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich 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 Zustimmung des Auftraggebers.

2.4 Art der Daten die der Auftraggeber speichert und dem Auftraggeber zur Kenntnis kommen können.
Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- ☑ Personenstammdaten
- ☑ weitere personenbezogene Daten, soweit vom Auftraggeber erfasst
- ☑ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☑ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☑ Kunden bzw. Klienten Historie
- ☑ Planungs- und Steuerungsdaten
- ☑ Auskunftsangaben (von Dritten, z.B. Adressen aus Telefonbüchern, Internetseiten)

2.5 Kategorien betroffener Personen
Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☑ Kunden (auch Klienten, Mitglieder, Spender, etc.)
- ☑ Interessenten
- ☑ Beschäftigte
- ☑ Personen in geschäftlicher Beziehung zum Auftraggeber
- ☑ Ansprechpartner

3 Technisch-organisatorische Maßnahmen

3.1 Der Auftragnehmer hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den 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. 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 im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen [Einzelheiten zu den technischen und organisatorische Maßnahmen stehen in den „Datenschutzrichtlinien zur Einhaltung der Vorgaben der DSGVO von SIT“ des Auftragnehmers und werden auf Anfrage zugesandt].

3.2 Die Umsetzung eines Auftrages durch den Auftragnehmer wird üblicherweise entsprechend der „Datenschutzrichtlinien zur Einhaltung der Vorgaben der DSGVO von SIT“ durchgeführt. Auf Anfrage des Auftraggebers können die technischen und organisatorischen Maßnahmen hinsichtlich der konkreten Auftragsdurchführung eines spezifischen Auftrags im Vorfeld der Auftragsvergabe dokumentiert werden. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

3.3 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4 Berichtigung, Einschränkung und Löschung von Daten

4.1 Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

4.2 Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

5.1 Der Auftragnehmer führt Wartungs- und/oder Pflegearbeiten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen.

5.2 Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- Gemäß Art. 38 und 39 DSGVO ist der Auftragnehmer nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Ansprechpartner beim Auftragnehmer ist Herr Hartmut Stricker, geschäftsführender Eigentümer des Auftragnehmers, Telefon: 07946-91510, E-Mail: info@stricker-it.de (oder Stellvertreter bei Abwesenheit).
- Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO.
- Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, 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 gesetzlich zur Verarbeitung verpflichtet sind.
- Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DSGVO [Einzelheiten stehen in den „Technisch-organisatorischen Maßnahmen“ des Auftragnehmers und werden auf Anfrage zugesandt].
- Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag 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.
- Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
- Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
- Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6 Unterauftragsverhältnisse

6.1 Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt.

6.2 Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

6.3 Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

6.4 Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

7 Kontrollrechte des Auftraggebers

7.1 Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

7.2 Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

7.3 Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, können auch durch Vorlage eines aktuellen Testats, von Berichten und Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren, etc.) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI Grundschutz) oder die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO erbracht werden.

7.4 Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8 Mitteilung bei Verstößen des Auftragnehmers

8.1 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

- die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die 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.
- die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
- die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
- die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
- die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

8.2 Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9 Weisungsbefugnis des Auftraggebers

9.1 Weisungen können schriftlich (z.B. E-Mail, Fax, etc.) oder mündlich gegeben werden. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

9.2 Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10 Löschung und Rückgabe von personenbezogenen Daten

10.1 Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

10.2 Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

10.3 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11 Geheimhaltung

11.1 Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

11.2 Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

12 Haftung

12.1 Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten bei der Erbringung der vertraglichen Leistung schuldhaft verursachen.

12.2 Für den Ersatz von Schäden, die eine betroffene Person wegen einer nach der DSGVO oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist der Auftraggeber gegenüber der betroffenen Person verantwortlich. Soweit der Auftraggeber zum Schadensersatz gegenüber der betroffenen Person verpflichtet ist, bleibt ihm der Rückgriff beim Auftragnehmer vorbehalten.

13 Sonstiges

13.1 Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen. Alle Daten, sind dem Auftraggeber in diesem Zusammenhang rechtzeitig vor Eintritt dieser Maßnahmen zu übergeben und von den betroffenen Datenverarbeitungsanlagen zu entfernen.

13.2 Die Einrede des Zurückbehaltungsrechts im Sinne des Privatrechts wird hinsichtlich der verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen.

14 Schlussbestimmungen

14.1 Die Unwirksamkeit einer Vertragsbestimmung berührt die Gültigkeit der übrigen Bestimmungen nicht. Sollte sich eine Bestimmung als unwirksam erweisen, werden die Vertragspartner diese durch eine neue ersetzen, die dem von den Parteien Gewollten am nächsten kommt.

14.2 Änderungen dieser Vereinbarung sowie Nebenabreden bedürfen der Schriftform. Dies gilt auch für das Abbedingen dieser Schriftformklausel selbst.

14.3 Es gilt deutsches Recht. Gerichtsstand ist der Sitz des Auftraggebers.

……..	Landesstelle d. Psychologischen Beratungsstellen, Augustenstr. 39B,70178 Stuttgart
Stuttgart, den 24.5.2018	Susanne Bakaus
(Ort, Datum)	(Auftraggeber)
Langenbrettach, 24.05.2018	SIT Stricker Informationstechnik Kirchberg 2 74243 Langenbrettach Tel. 07946-91510 · Fax 915130
(Ort, Datum)	(Auftragnehmer)