Vereinbarung zur Auftragsverarbeitung
nach Art. 28 DS-GVO

zwischen

Vorname, Name / Einrichtung:
Straße:
PLZ, Ort:
LANR:

- Verantwortlicher im Sinne der DS-GVO -
nachstehend Auftraggeber genannt -

und
Technik und IT in der ärztlichen und psychotherapeutischen Praxis
–Tech-Prax GmbH
Donnerschweer Str. 398
26123 Oldenburg

- Auftragsverarbeiter im Sinne der
- Auftragsverarbeiter im Sinne der DS-GVO -
nachstehend Auftragnehmer genannt

Präambel

Dieser Auftragsverarbeitungs-Vertrag (AV-Vertrag) konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der im Vertrag

Dienstleistungsvertrag für IT Dienstleistung per Fernwartung

Und/Oder

Dienstleistungsvertrag für Firewall-Lösungen

Und/Oder

Einmaliger Fernwartungen

Und/Oder

Nutzung Sicherheitssoftware / Komplettpaket Hardware

Und/Oder

Monitoring und Patchmanagement

(im Folgenden Hauptvertrag genannt) beschriebenen Auftragsverarbeitung ergeben. Sämtliche in diesem Vertrag beschriebenen Verpflichtungen finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen bzw. kommen können. Alternativ für die Durchführung von IT-Dienstleistungen und PC-Einrichtungen, welche auf Honorarbasis abgerechnet werden und nicht Bestandteil eines Wartungsvertrages sind.

1. Gegenstand und Dauer des Auftrags

Der Auftragnehmer verarbeitet personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Vertrages.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

1.1 Gegenstand der Vereinbarung

Die Vereinbarung bezieht sich auf die Wartungs- und Supporttätigkeiten und PC Einrichtungen in Bezug auf die EDV Betreuung und der Telematikinfrastruktur über die Fernwartung und den vor Ort Service. Zudem werden Sicherheitslösungen (Firewall / Antivirenssoftware) von Securepoint &/ Kaspersky eingesetzt und ein Monitorung und Patchmanagement auf Kundenwunsch durch Server Eye durchgeführt.

Die Benutzung einer Fernwartungssoftware wird für die Wartungstätigkeit und Einrichtung von Hard-ware und Software der entsprechenden EDV Analgen durchgeführt. Mit Start der Fernwartungssoftware z.Z. „Teamviewer“ gestattet der Auftraggeber einem Mitarbeiter des Auftragnehmers die Einsicht und die Fernsteuerung des PCs mit der Möglichkeit der Datenveränderung.

1.2 Dauer des Auftrags

Die Dauer dieses Auftrags (Laufzeit) entspricht dem im Hauptvertrag definierten Zeitraum zur Leistungserbringung und beginnt mit dem Datum der Unterschrift. Dieser Vertrag endet automatisch mit der Beendigung des Hauptvertrags. Sollte kein Wartungsvertrag geschlossen werden, so läuft dieser Auftragsdatenverarbeitungsvertrag bis zur Kündigung dieses Vertrages. Bei Sicherheitssoftware endet dieser Vertrag mit Kündigung der entsprechenden Sicherheitssoftware Lösung.

2. Konkretisierung des Auftragsinhalts

2.1 Art und Zweck der vorgesehenen Verarbeitung von Daten

Die Verarbeitung dient den unter Nr. 1 dieser Vereinbarung beschriebenen Tätigkeiten. Anlässlich dieser Tätigkeiten unterstützt der Auftragnehmer den Auftraggeber insbesondere dabei, die auftretenden EDV Probleme / Aufträge zu:

- zu installieren,

- zu konfigurieren,

- seine Funktionalität zu erhalten bzw. wiederherzustellen,

- Schulungen durchzuführen

- Sicherheitsniveaus zu erhöhen

- Monitoring der PC Daten

- Patchmanagement

Die Verarbeitung dient folgendem Zweck:
Art und Zweck des Vertrages umfasst die Wartungs- und Supporttätigkeiten in Bezug auf die EDV Praxisbetreuung und Sicherheitslösungen. Des weiteren beinhaltet dieses die Einrichtung und Wartung der Telematikinfrastruktur. 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 ist ausgeschlossen.

2.2 Art der Daten

Gegenstand der Erhebung, Verarbeitung und / oder Nutzung sind personenbezogene Daten, die sowohl Kundendaten (Personenstammdaten oder ähnliches) als auch Patientendaten umfasst.

Gegenstand der Verarbeitung können insbesondere sein:

- Personenstammdaten des Kunden
- Kommunikationsdaten (z.B. Telefon, E-Mail) des Kunden
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse) des Kunden
- Kundenhistorie des Kunden
- Vertragsabrechnungs- und Zahlungsdaten des Kunden
- Mitarbeiterdaten des Kunden
- besondere personenbezogene Daten (Patientendaten), insbesondere
    - Gesundheitsdaten, genetische Daten, biometrische Daten
- Sicherheitsdaten der Securepoint Firewall oder des Securepoint Antivirenprogrammes
    - IP-Adresse
    - Personenstammdaten des Kunden
    - Rechnername
    - Lizenzdaten
    - Virusmeldungen
    - Systemstatus
- Server Eye Monitoring und Patchmanagement
    - Abhängig von der Art der installierten Sensoren werden Personenstammdaten und Kommunikationsdaten zusammen mit den Betriebsdaten der überwachten Hardware bzw. Software verarbeitet.
    -

2.3 Kategorien betroffener Personen

Kategorien im Rahmen dieser Vereinbarung betroffenen Personen sind insbesondere:

- Kunden und Interessenten des Auftragnehmers
- Geschäftsleitung und Beschäftigte des Auftragnehmers
- Ehemalige Beschäftigte des Auftragnehmers
- Patienten des Auftraggebers

3. Technisch-organisatorische Maßnahmen

1) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO 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 DS-GVO zu berücksichtigen [Einzelheiten in Anlage].

2) 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

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.

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

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

1) Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche

Pflichten gemäß Artt. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art.38 und 39 DS-GVO ausübt:

Als Datenschutzbeauftragter ist beim Auftragnehmer
Herr Eugen Pernizki, Donnerschweer Straße 398, 26123 Oldenburg bestellt.
Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. 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.

Der Auftragnehmer wirkt als Dienstleister an der beruflichen Tätigkeit des Auftraggebers, der einer beruflichen Verschwiegenheitsverpflichtung unterliegt, mit. Der Auftragnehmer wahrt in Kenntnis der strafrechtlichen Folgen einer Verletzung der Verschwiegenheitspflicht gemäß § 203 StGB und den sonst anwendbaren rechtlichen Vorschriften fremde Geheimnisse, die ihr von dem Auftraggeber zugänglich gemacht werden.

Der Auftragnehmer verpflichtet sich, sich nur insoweit Kenntnis von fremden Geheimnissen zu verschaffen, als dies zur Vertragserfüllung erforderlich ist.

Die Pflicht zur Verschwiegenheit besteht nicht, soweit der Auftragnehmer auf Grund einer behördlichen oder gerichtlichen Entscheidung zur Offenlegung von vertraulichen Informationen des Auftraggebers verpflichtet ist. Soweit dies im Einzelfall zulässig und möglich ist, wird der Auftragnehmer den Auftraggeber über die Pflicht zur Offenlegung vorab in Kenntnis setzen.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage].

d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) 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.

f) 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.

g) 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.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 8 dieses Vertrages.

2) Der Auftragnehmer unterstützt angesichts der Art der Verarbeitung nach Möglichkeit den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Ansprüche der betroffenen Personen nach Kapitel III der DSGVO. Der Auftragnehmer ist berechtigt, für diese Leistungen eine angemessene Vergütung vom Auftraggeber zu verlangen.

6. Rechte und Pflichten des Auftraggebers

1) Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die

Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

2) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

3) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

4) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

5) Der Auftraggeber hat stets die aktuelle lizenzierte Version der vertragsgegenständlichen Software zu nutzen. Zur Fehleranalyse durch die Tech-Prax GmbH hat der Auftraggeber den Fehler möglichst genau zu beschreiben und ggf. Screenshots oder eine Datensicherung (Datenbank) bereit zu stellen.

8) Der Auftraggeber hat seine Datenbestände und EDV-Anlagen durch geeignete organisatorische und technische Vorkehrungen wie z.B. Virenscanner, Firewalls und Passwortschutz ausreichend zu schützen. Der Auftraggeber trägt selbst die Verantwortung für eine aktuelle Datensicherung in angemessener Form. Es gehört zu den Obliegenheiten des Auftragsgebers sicherzustellen, dass Daten mindestens kalendertäglich durch Sicherungskopien gesichert werden. Diese Sicherung muss auch eine zeitnahe und wirtschaftlich vernünftige Wiederherstellung der Daten garantieren.

9) Der Auftraggeber hat sicherzustellen, dass die Verarbeitung und Nutzung von personenbezogenen Daten auf seinen EDV-Anlagen unter Beachtung der DS-GVO erfolgt. Insbesondere hat der Auftraggeber während der Fernwartungssitzung dafür zu sorgen, dass er selbst oder eine von ihm autorisierte Person die Fernwartungssitzung auf dem Bildschirm in der Praxis überwacht. Die Überwachungsperson des Auftraggebers kann die aktuelle Fernwartungssitzung jederzeit durch Schließen der Fernwartungssoftware beenden. Erfährt ein Mitarbeiter der Tech-Prax GmbH im Laufe der Fernwartung sicherheitsrelevante Kennwörter, hat der Auftraggeber diese sofort nach Beendigung der Fernwartung zu ändern.

7. Unterauftragsverhältnisse

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. 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.

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

b) Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu, unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

Firma Unterauftragnehmer	Anschrift	Leistung
Securepoint GmbH	Bleckeder Landstr. 28 21337 Lüneburg	Managed Firewall Lösungen und managed Antivirus Pro
Krämer IT Solutions GmbH	KoßmannStr.7 66571 Eppelporn	Server Eye Monitoring und Patchmanagement

c) Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und

- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und

- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

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

4) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

8. Kontrollrechte des Auftraggebers

1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennendem 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.

2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO 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.

3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO.

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

9. Mitteilung bei Verstößen des Auftragnehmers

1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 33 bis 34 der DS-GVO genannten Pflichten, hierzu gehören u.a.

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
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
c) 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
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

10. Weisungsbefugnis des Auftraggebers

1) Mündliche Weisungen werden in der Kundenverwaltung beim Auftragnehmer schriftlich dokumentiert.

2) Der Auftragnehmer hat den Auftraggeber 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.

11. Löschung und Rückgabe von personenbezogenen Daten

1) Es werden Sicherheitskopien erstellt, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

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.

3) Dokumentationen, die dem Nachweis der auftrags-und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

12. Informationspflichten, Schriftformklausel

1) 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. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit an den Daten beim Auftraggeber liegt.

2) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile -einschließlich etwaiger Zusicherungen des Auftragnehmers -bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

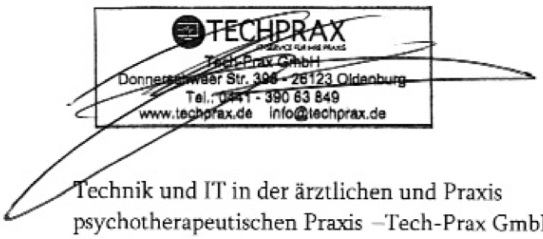
13. Salvatorische Klausel

Sollten einzelne Bestimmungen dieser Zusatzvereinbarung unwirksam oder undurchführbar sein

oder nach Unterzeichnung unwirksam oder undurchführbar werden, bleibt davon die Wirksamkeit dieser Vereinbarung im Übrigen unberührt.

Oldenburg, 04.09.2020

Ort/Datum/Stempel, Unterschrift



Technik und IT in der ärztlichen und Praxis
psychotherapeutischen Praxis –Tech-Prax GmbH
(Auftragnehmer)

Ort/Datum/Stempel, Unterschrift

Praxis
(Auftraggeber)

Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 DSGVO

der Organisation

Technik und IT in der ärztlichen und psychotherapeutischen Praxis
–Tech-Prax GmbH

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Die oben genannte Organisation erfüllt diesen Anspruch durch folgende Maßnahmen:

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

1.1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Technische Maßnahmen	**Organisatorische Maßnahmen**
- Geschäftsräume sind durch zwei Türen gesichert	- Schlüsselregelung / Liste
- Manuelles Schließsystem	- Besucher nur in Begleitung durch Mitarbeiter
- Türen mit Knauf auf Außenseite	- Sorgfalt bei Auswahl der Reinigungsdienste
- Klingelanlage mit Kamera	- Geschäftsräume werden nur zu Geschäftszeiten betreten
- Chipkarten / Transpondersysteme	- Besucher Listen mit Unterschrift

1.2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können. Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint.

Technische Maßnahmen	**Organisatorische Maßnahmen**
- Login mit Benutzername und Passwort	- Verwaltung von Benutzerberechtigungen
- Anti-Viren-Software Server	- Zentrale Passwortvergabe
- Anti-Viren-Software Clients	- Richtlinie „Sicheres Passwort“
- zwei unabhängige Firewalls	- Richtlinie „Löschen / Vernichten“
- Server sind nur per VPN Verbindung von außen erreichbar, nur von autorisierten Mitarbeitern	- Allgemeine Richtlinie Datenschutz und / oder Datensicherheit
- Verschlüsselung von Festplatten (Server und Clients)	- Wartungs- und Reparaturarbeiten werden nur durch ausgewählte Fachfirmen durchgeführt

1.3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Technische Maßnahmen	**Organisatorische Maßnahmen**
- Aktenschredder, Sicherheitsstufe P4 cross cut	- Einsatz von Berechtigungskonzepten
- Datenschutzkonforme Vernichtung / Löschung von Daten	- Minimale Anzahl an Administratoren
- Sichere Aufbewahrung von Datenträgern / Datensicherungen	- Verwaltung von Benutzerrechten durch Administratoren

1.4. Trennungskontrolle

Es wird gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden und zwar durch eine logische sowie physikalische Trennung.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports 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.

Die Weitergabe der pd-Daten betrifft den Auftragnehmer nur intern. Eine Weitergabe an Dritte Einrichtungen findet nicht statt.

Technische Maßnahmen	**Organisatorische Maßnahmen**
- technische Protokollierung bei Datenempfang, Weitergabe und Löschung	- Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. Löschfristen
- technisches Berechtigungskonzept durch den Server für Datenempfänger	- nur autorisierte Mitarbeiter werden als Datenempfänger benannt
- Verschlüsselung von Festplatten (Server und Clients)	- die Weitergabe der Daten erfolgt ausschließlich über den internen Server
- die Weitergabe der Daten erfolgt ausschließlich über den internen Server	

2.2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können.

Technische Maßnahmen	**Organisatorische Maßnahmen**
- technische Protokollierung der Eingabe, Änderung und Löschung von Daten	- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen
	- nur autorisierte Mitarbeiter dürfen pb-Daten verändern und löschen
	- die Eingabe, Änderung und Löschung findet nur in einem Programm statt, dem Kundensupport-Programm

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

3.1. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.

Technische Maßnahmen	**Organisatorische Maßnahmen**
- Feuer- und Rauchmeldeanlagen	- Backup und Recovery Konzept
- Feuerlöscher im Serverraum	- Server Datensicherungen werden extern aufbewahrt
- Serverraum ist klimatisiert	- Getrennte Partitionen für OS und Daten
- Schutzsteckdosenleisten im Serverraum	- keine sanitären Anschlüsse im oder oberhalb des Serverraums
- USV	
- RAID System	
- Anti-Viren-Software Server	
- Anti-Viren-Software Clients	

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGV)

4.1. Datenschutz-Management

Technische Maßnahmen	**Organisatorische Maßnahmen**
- Software-Lösungen für Datenschutz-Management im Einsatz	Interner Datenschutzbeauftragter: Eugen Pernizki Donnerschweer Straße 398 26123 Oldenburg Tel.: 0441 - 390 112 00 e-Mail: datenschutz@newmediacompany.de
- Datenschutz Konzepte für die Verarbeitung der pb-Daten	- Mitarbeiter sind geschult und auf Vertraulichkeit und Datengeheimnis verpflichtet
- Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz, mit Zugriffsmöglichkeiten für Mitarbeiter	- Regelmäßige Sensibilisierung der Mitarbeiter
- Eine Überprüfung der Wirksamkeit der TOM wird regelmäßig durchgeführt	- Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DS-GVO nach
	- Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden
	- eine Datenschutzfolgeabschätzung wurde und wird fortlaufend durchgeführt

4.2. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Es werden nicht mehr personenbezogene Daten erhoben, als für den Zweck erforderlich sind.