Vertrag über eine Auftragsverarbeitung gemäß Art. 28 DSGVO

zwischen dem/der Kunden:in der psyprax GmbH
Praxis/BAG/MVZ/Institut/PiA

.....

.....

.....

.....
(Praxisinhaber:in)

Zusätzliche Weisungsbefugte:

.....

.....

.....
- Verantwortlicher - nachstehend Auftraggeber genannt –
und der
psyprax GmbH
Landsberger Str. 308
80687 München

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

MUSTER

1 Gegenstand und Dauer des Auftrags

1.1 Gegenstand des Auftrags

Der Gegenstand des Auftrags ergibt sich aus dem jeweiligen geschlossenen Vertrag.

Die Fernwartungen werden durch den Auftraggeber oder den Auftraggeber weisungsbefugten Personen gestartet. Der Auftragnehmer kann sich nicht ohne Wissen des Auftraggebers einwählen.
In Ausnahmen besteht im Supportfall die Möglichkeit, dass unsere Entwickler oder das Produktmanagement die notwendigen Datenbanken direkt beim Kunden über die Fernwartung holen.

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. DSGVO erfüllt sind.

1.2 Dauer des Auftrags

a) Der Vertrag beginnt mit Vertragsabschluss.
b) Der Vertrag endet automatisch mit der Beendigung des Softwarewartungsvertrags.
c) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

2 Konkretisierung des Auftragsinhalts

2.1 Art und Zweck der Verarbeitung von personenbezogenem Daten

Art und Zweck der Verarbeitung personebezogener Daten durch den Auftragnehmer für den Auftragnehmer ergeben sich aus dem jeweilig geschlossenen Vertrag.

2.2 Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- Personenstammdaten
- Kommunikationsdaten
- Identifikationsdaten
- Rechnungsdaten
- IP-Adressen
- Kundenhistorie

MUSTER

2.3 Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Patientendaten des Auftraggebers
- Mitarbeiterdaten des Auftragsgebers
- Dienstleister des Auftragsgeber
- Sonstige Daten von Dritten, die vom Auftraggeber beim Fernwartung offenbart werden

3 Technisch-organisatorische Maßnahmen

3.1 Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. 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.

3.2 Der Auftragnehmer hat die Sicherheit gem. Art. 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 [Anlage 1 – technisch organisatorische Maßnahmen (TOMs].

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 Rechte von betroffenen Personen

4.1 Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich mittels geeigneter technisch-organisatorischer Maßnahmen bei der Beantwortung und Umsetzung von Anträgen betroffener Personen hinsichtlich ihrer Datenschutzrechte. Er darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers beauskunften, portieren, 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.

MUSTER

4.2 Soweit vom Leistungsumfang umfasst, sind die Rechte auf Auskunft, Berichtigung, Einschränkung der Verarbeitung, Löschung sowie Datenportabilität nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5 Pflichten des Auftraggebers

5.1 Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO 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.

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

5.3 Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

5.4 Der Auftraggeber ist berechtigt, sich wie unter Nr. 3 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

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

5.6 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.

6 Datengeheimnis/Qualitätssicherung und sonstige Pflichten des Auftragnehmers

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

a. Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

b. Die Wahrung der Vertraulichkeit gemäß Art. 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

MUSTER

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.

c. Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO [Anlage 1 – technisch organisatorische Maßnahmen (TOMs)].

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.

6.2 Dieser Vertrag entbindet den Auftragnehmer nicht von der Einhaltung anderer Vorgaben der DSGVO.

7 Unterauftragsverhältnisse

7.1 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 in Anspruch nimmt, z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Reinigungsleistungen oder Bewachungs-dienstleistungen. Wartungs- und Prüfleistungen stellen dann ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die im Zusammenhang mit einer Leistung des Auftragnehmers nach diesem Vertrag erbracht werden. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftrag-gebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

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

a) ☐ Eine Unterbeauftragung ist unzulässig.

b) ☒ Der Auftraggeber stimmt der Beauftragung der in Anhang 2 bezeichneten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO mit dem Unterauftragnehmer zu.

MUSTER

Die vertragliche Vereinbarung wird dem Auftraggeber auf dessen Verlangen vorgelegt, wobei geschäftliche Klauseln ohne datenschutzrechtlichen Bezug hiervon ausgenommen sind.

c) ☐ Die Auslagerung auf Unterauftragnehmer oder

☒ der Wechsel der gemäß Anhang 2 bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber in einer angemessenen Zeit, die 14 Tage nicht unterschreiten darf, 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.

7.3 Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. Die Einhaltung und Umsetzung der technisch-organisatorischen Maßnahmen beim Unterauftragnehmer wird unter Berücksichtigung des Risikos beim Unterauftragnehmer vorab der Verarbeitung personenbezogener Daten und sodann regelmäßig durch den Auftragnehmer kontrolliert. Der Auftragnehmer stellt dem Auftraggeber die Kontrollergebnisse auf Anfrage zur Verfügung. Der Auftragnehmer stellt ferner sicher, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Kontrollrechte) auch direkt gegenüber den Unterauftragnehmern wahrnehmen kann.

7.4 Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt wer-den sollen.

7.5 Eine weitere Auslagerung durch den Unterauftragnehmer ist nicht gestattet.

8 Kontrollrechte des Auftraggebers

8.1 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.

8.2 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.

MUSTER

8.3 Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

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

9 Mitteilung bei Verstößen des Auftragnehmers

9.1 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.

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

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

10 Weisungsbefugnis des Auftraggebers

10.1 Der Auftragnehmer verarbeitet personenbezogene Daten nur auf Basis dokumentierter Weisungen des Auftraggebers, es sei denn er ist nach dem Recht des Mitgliedstaats oder nach Unionsrecht zu einer Verarbeitung verpflichtet. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform). Die anfänglichen Weisungen des Auftraggebers werden durch diesen Vertrag festgelegt. Mündliche Weisungen werden beim Auftragsnehmer in der Kundenverwaltung dokumentiert.

MUSTER

10.2 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 so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

11 Löschung und Rückgabe von personenbezogenen Daten

11.1 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.

11.2 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.

11.3 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.

12 Haftung

12.1 Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffener Regelung.

MUSTER

_____ _____

Unterschrift Auftraggeber Unterschrift Auftragnehmer

_____

Datum

Anlage 1
Technisch-organisatorische Maßnahmen

1 Vertraulichkeit (Art. 32 Abs. 1 lit b DSGVO)

1.1 Zutrittskontrolle

- Kein unbefugter Zutritt zu Datenverarbeitungsanlagen durch neutrale Chipkarten.
- Dokumentierte Schlüsselvergabe und Chipkartenvergabe an Mitarbeiter.
- Der Zutritt zu den Serverräumen ist nur dem Administrator und der Geschäftsleitung
- Elektronisches Zutrittskontrollsystem mit Protokollierung und mit Gegensprechanlage für Besucher.
- Der Zutritt für betriebsfremde Personen (Besucherinnen und Besucher) zu den Räumen ist wie folgt beschränkt: nur in Begleitung eines psyprax GmbH Mitarbeiters.
- Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude.
- Der Auftragnehmer trägt Sorge dafür, dass seine Büro- und Geschäftsräume grundsätzlich außerhalb der Büro- und Geschäftszeiten geschlossen sind.
- Die Firmenräume sind mit Sicherheitsschlössern versehen.
- Videoüberwachung an Ein- und Ausgängen obliegt der Hausverwaltung.
- Sorgfältige Auswahl von Reinigungspersonal.

1.2 Zugangskontrolle

- Der Login zu Datenverarbeitungslagen wird über eine Firewall, Benutzername und Passwort kontrolliert.
- Für Remotemitarbeiter ist darüber hinaus ein VPN Zugang zwingend (dieser wird jedem Mitarbeiter bereitgestellt).
- Des Weitern wird auf den Servern und Clients eine aktuelle Endpoint Security Software verwendet.
- Die Firewall wird regelmäßig gewartet und an neue Anforderunen angepasst.
- Es besteht eine zentrale Benutzerverwaltung (Windows Active Directory).
- Zugriffe auf Datenverarbeitungsanlagen werden protokolliert.
- Zwei-Faktor Authentifizierung (in einigen Bereichen)
- Die Nutzung von Notebooks wurde schriftlich geregelt und wird regelmäßig durch die Geschäftsleitung geprüft sowie durch geeignete Überwachungssysteme (Firmeneigene Software).
- Notebooks und Desktop-PCs werden dezentral mit Bitlocker verschlüsselt. Andere mobile Datenträger sind nicht im Einsatz.
- Nicht mehr verwendete Datenträger werden durch eine Richtlinie „Löschen/Vernichten“ sichergestellt.
- Keine unbefugte Systembenutzung und der Zugang ist passwortgeschützt, Zugriff besteht nur für berechtigte Mitarbeiter; verwendete Passwörter entsprechen der Richtlinie „Passwortrichtlinie“ und werden in Bedarfsfall erneuert.
- Alle Mitarbeiter sind angewiesen, ihre IT-Systeme zu sperren, wenn sie den Arbeitsplatz verlassen.

1.3 Zugriffskontrolle

- Es wird darauf geachtet nur eine minimale Anzahl an Administratoren im Unternehmen zu haben.

MUSTER

- Die Verwaltung von Benutzerrechten und Benutzergruppen erfolgt ausschließlich durch die Admistratoren.
- Papierunterlagen mit personenbezogenen Daten werden mittels elektrischer Aktenvernichter (Klasse 3) sicher vernichtet, sowie durch datenschutzkonforme Entsorgung über externe Aktenvernichter (Akten, Laufwerke etc.) inkl. Dokumentation.
- Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, durch Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten.

1.4 Trennungskontrolle

- Bei internen Verwaltungssystemen werden die Daten physisch oder logisch von anderen Daten getrennt und abgespeichert.
- Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.
- Die Steuerung erfolgt über Berechtigungskonzepte sowie wie über Datenbankrechte.

1.5 Pseudonymisierung

- Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfirst möglichst zu anonymisieren/ pseudonymisieren

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

2.1 Weitergabekontrolle

- Alle externen Mitarbeiter werden via VPN an die Server angeschlossen, dabei werden Zugriffe und Abrufe protokolliert.
- Alle Emails werden via S/MIME verschlüsselt und versendet, sofern die Gegenseite dies unterstützt.
- Die Bereitstellung der Fernwartung, Websites wird über verschlüsselte Verbindungen via https gewährleistet.
- Die Nutzung von privaten Datenträgern wie USB-Sticks, externe Festplatten sind untersagt.

2.2 Eingabekontrolle

- Bei internen Verwaltungssystemen ist eine Nachvollziehbarkeit von Eingabe, Änderung und Löschung der Daten durch individuelle Benutzer gegeben.
- Die Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten passiert auf Basis des Berechtigungskonzeptes, sowie einer klaren Definition der Zuständigkeit für Löschungen.

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

MUSTER

3.1 Verfügbarkeitskontrolle

- Im Bürogebäude sind Feuer- und Rauchmeldeanlagen verbaut, sowie Feuerlöscher im Gang und in den Serverräumen vorhanden.
- Die Serverräume Verfügungen über eine Klimaanlage sowie über eine Überwachungsanlage für die Temperatur und Feuchtigkeit. In den Serverräumen sind USV sowie Schutzsteckdosenleisten verbaut. Die Server verfügen über ein RAID-System.
- Getrennte Partionen für Betriebssysteme und Daten
- Zusätzlich ist ein Backup- und Recovery-Konzept vorhanden, welches in regelmäßigen Abständen auf Wiederherstellbarkeit der Daten (alle 6 Monate) geprüft wird.
- Die Sicherungen des Servers werden außerhalb des Servers aufbewahrt. Die Architektur des Bürohauses ist so gestaltet, dass keine Sanitären Anlagen oberhalb des Serverraums vorzufinden sind.
- Notfallmanagement

3.2 Wiederherstellbarkeit

- Notfall-Management

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

4.1 Datenschutzmanagement

- Bestellung eines externen Datenschutzbeauftragten (wird auf der Internetseite veröffentlicht)
- Zentral sind alle Verfahrensweisen und Regelungen zum Datenschutz abgelegt und für alle Mitarbeiter nach Bedarf zugänglich.
- Jährlich findet eine Sensibilisierung zum Datenschutz und Awarenessschulungen statt. Ebenfalls wird jährlich die Wirksamkeit der technischen Schutzmaßnahmen überprüft.
- Mitarbeiter werden auf die Vertraulichkeit und das Datengeheimnis verpflichtet
- Datenschutzfolgeabschätzungen werden nach Bedarf mit dem interen und exteren Datenschutzbeauftragten durchgeführt.
- Prozess zur Bearbeitung von Auskunftsersuchen von Betroffenen ist vorhanden
- Die Firma kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach.
- Ein Informationssicherheitskonzept angelehnt an die ISO 27001vorhanden

4.2 Incident-Response-Management

- Zum Schutz der Daten ist eine Hardware Firewall, ein Spamfilter, Virenscanner im Einsatz, welche regemäßig aktualisiert werden.
- Sicherheitsvorfälle und Datenpannen werden via Ticketsystem dokumentiert.
- Bei Sicherheitsvorfällen und Datenschutzpannen werden die Datenschutzbeauftragten und der Informationssicherheitsbeauftragte eingebunden.

MUSTER

4.3 Datenschutzfreundliche Voreinstellungen (Art. 35 Abs. 2 DSGVO)

- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.
- Die Speicherung der Daten wird begrenzt – Löschkonzept – gesetzliche Regelung werden umgesetzt.
- Beschränkung der Zugänglichkeit der Daten – wenn der Löschzeitpunkt noch nicht erreicht wurde.
- Einfache Ausübung des Wiederrufrechts des Betroffenen durch technische Maßnahmen.

4.4 Auftragskontrolle

- Die Einbindung von externen Dienstleistern, welche unter Umständen personenbezogene Daten des Auftraggebers zur Kenntnis nehmen können, ist nur nach sorgfältiger Prüfung durch den Datenschutzbeauftragten und Abschluss eines Auftragsverarbeitungsvertrages bzw. EU-Standarddardvertragsklauseln gemäß Artikel 28 DSGVO zulässig. (insbesondere wird den Datenschutz und die Datensicherheit geprüft).
- Die externen Dienstleister versichern ihre Mitarbeiter auf die Vertraulichkeit und das Datengeheimnis zu verpflichten.

MUSTER

Anlage 2
Unterauftragnehmer

Firma Unterauftragnehmer	Anschrift/Land	Leistung
KoSyMa GmbH	Große Hub 7c 65344 Eltville am Rhein	VPN-Zugangsdienst KIM+ und KIM 1.5
MEDKONNEKT GmbH	Schleißheimer Straße 91 A 85748 Garching b. München	TI-Gateway
Securepoint GmbH	Bleckeder Landstraße 28 21337 Lüneburg	IT-Dienstleister
CROWDSTRIKE GMBH c/o Digitevo Deutschland GmbH	Felsweg 4 35435 Wettenberg	IT-Dienstleister
Samhammer AG	Zur Kesselschmiede 3 92637 Weiden in der Oberpfalz	IT-Dienstleister
PowerBit	Sudetenlandstr. 31 80687 München	IT-Dienstleister
SL.IS Services GmbH	Konrad-Adenauer-Allee 44 64569 Nauheim	IT-Dienstleister
IF-Blueprint AG	Truderinger Straße 265 81825 München	IT-Dienstleister
mioso – IT-Solutions	Jarresstraße 42 22303 Hamburg	IT-Dienstleister
Wortmann AG	Bredenhop 20 32609 Hüllhorst	Infrastrukturkomponenten
eHealths Experts GmbH	Emil-Figge-Straße 85 44227 Dortmund	Softwareentwicklung
Terra Cloud GmbH	Hankamp 2 32609 Hüllhorst	Hosting
Salesforce.com Germany GmbH	Erika-Mann-Str. 31 80636 München	Ticketsystem
knowhere GmbH	Karolinenstraße 9 20357 Hamburg	Chatbot MoinAI
Rapidmail GmbH	Augustinerplatz 2 79098 Freiburg	Newsletter Versand
CleverReach GmbH & Co. KG	Schafjückenweg 2 26180 Rastede	Newsletter Versand
Datev	Virnsberger Straße 63 90431 Nürnberg	Buchhaltung
DIABOLOCOM GmbH	Savignystr. 43 60325 Frankfurt	Telefonie
WebDevel e.K.	Im Sonnenland 4 65760 Eschborn	Hosting
KoSyMa Services GmbH	Große Hub 7c 65344 Eltville am Rhein	TI-Gateway
R&R IT Solutions	Bahnhofstr. 55 04552 Borna	IT-Dienstleister

MUSTER