Vertrag über die Auftragsverarbeitung personenbezogener Daten i. S. d. Art. 28 Abs. 3 EU-Datenschutzgrundverordnung (EU-DSGVO)

zwischen

_____

im Folgenden – Auftraggeber - genannt

und

Firma
Praxis der Zukunft® GmbH
vertreten durch die Geschäftsführerin Sigrid Borst
Vaihinger Str. 95
70567 Stuttgart
Telefon: 0178-8127359
Fax: 03213-1394863
E-Mail: kontakt@hzv-abrechnung.de
Webseite: www.hzv-abrechnung.de

im Folgenden – Auftragnehmer - genannt

§ 1 Präambel

(1) Der Auftragnehmer erbringt für den Auftraggeber Beratungs- und Unterstützungsleistungen im Bereich Optimierung der ärztlichen Abrechnung.

(2) Bei der Leistungserbringung des Auftragnehmers wird der Auftragnehmer potentiell mit personenbezogenen Daten in Berührung kommen, die der Auftraggeber als Verantwortlicher im Sinne der Verordnung (EU) 2016/679 („EU-DSGVO“) verarbeitet.

(3) Mit diesem Vertrag wollen die Parteien sicherstellen, dass der Auftragnehmer seine Leistungen als Auftragsverarbeiter erbringt, indem er im Sinne von Art. 28 Abs. 3 S. 1 EU-DSGVO an den Auftraggeber gebunden wird.

§ 2 Gegenstand und Dauer der Auftragsverarbeitung

(1) Die Auftragsverarbeitung erfolgt durch den Auftragnehmer als weisungsgebundene Tätigkeit nach Maßgabe der nachstehenden Vereinbarungen im Auftrag des Auftraggebers. Gegenüber den betroffenen Personen und Dritten trägt allein der Auftraggeber die Verantwortung für die Zulässigkeit der in seinem Auftrag durchgeführten Verarbeitungen personenbezogener Daten.

(2) Der Gegenstand des Auftrags ist die Erbringung der Leistungen und die Durchführung der mit diesen Leistungen zusammenhängenden Verarbeitungen personenbezogener Daten sind in Anhang 1 beschrieben.

(3) Der Vertrag wird auf unbestimmte Zeit geschlossen. Die Kündigungsfrist beträgt 4 Wochen zum Monatsende.

§ 3 Beschreibung der Auftragsverarbeitung

(1) Die Art und der Zweck der Auftragsverarbeitung sind in Anhang 1 beschrieben.

(2) Die Art der Daten und die Kategorien betroffener Personen sind in Anhang 1 beschrieben.

§ 4 Allgemeines zu den Rechten und Pflichten des Auftraggebers

(1) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn der Auftraggeber Fehler oder Unregelmäßigkeiten bei der Prüfung der

Auftragsverarbeitung, gelegentlich bei der Kontrolle nach „§ 10 Prüf-, Zutritts- und Auskunftsrechte des Auftraggebers“ oder auf andere Weise feststellt.

(2) Bei Ausübung seiner Befugnisse aus diesem Vertrag nimmt der Auftraggeber Rücksicht auf die Rechte, Rechtsgüter und Interessen des Auftragnehmers.

§ 5 Weisungsrecht des Auftraggebers

(1) Der Auftragnehmer verpflichtet sich, die Auftragsverarbeitung grundsätzlich nur nach den vertraglichen Vorgaben durchzuführen, die der Auftraggeber im Einzelfall durch Weisungen konkretisieren kann. Dem Weisungsrecht unterliegt die Entscheidung, ob eine Verarbeitung stattfindet und welche Daten durch den Auftragnehmer verarbeitet werden. Die Entscheidung über die Mittel der Verarbeitung trifft allein der Auftraggeber, indes besteht eine vertragliche Pflicht zur Ausführung der Verarbeitung mit bestimmten Mitteln oder auf bestimmte Art und Weise nur nach vorheriger Einigung der Parteien, die auch die entsprechende Gegenleistung des Auftraggebers umfasst. Das Weisungsrecht erstreckt sich nicht auf die vom Auftragnehmer zu ergreifenden technischen und organisatorischen Maßnahmen und findet im Allgemeinen seine Grenzen in den Vereinbarungen dieses Vertrags.

(2) Weisungen für die Auftragsverarbeitung hat der Auftraggeber dem Auftragnehmer mindestens in Textform mitzuteilen und ihre Erteilung zu dokumentieren. Weisungen muss der Auftraggeber an die Geschäftsleitung des Auftragnehmers oder an einen von dieser in Anhang 1 benannten Weisungsempfänger richten. Weisungsbefugt sind die Geschäftsleitung des Auftraggebers sowie jeder von dieser zu diesem Zweck ermächtigten Mitarbeiter des Auftraggebers.

(3) Der Auftragnehmer muss den Auftraggeber darauf hinweisen, wenn eine Weisung des Auftraggebers nach Ansicht des Auftragnehmers gegen geltendes Datenschutzrecht verstößt (Beanstandung). Der Auftragnehmer ist berechtigt, die Durchführung einer beanstandeten Weisung solange auszusetzen, bis der Auftraggeber die beanstandete Weisung überprüft und gegenüber dem Auftragnehmer als auszuführende Weisung bestätigt hat. Auch eine Bestätigung ist nur wirksam, wenn sie mindestens in Textform mitgeteilt wird und ihre Erteilung ist ebenfalls vom Auftraggeber zu dokumentieren.

(4) Der Auftragnehmer ist zu Verarbeitungen jenseits der vertraglichen Vorgaben berechtigt, sofern der Auftragnehmer durch das Recht der Europäischen Union oder des Mitgliedstaates, dem Auftragnehmer unterliegt, hierzu verpflichtet ist. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Vornahme einer solchen Verarbeitung mit, sofern das

betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

§ 6 Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer setzt für die Datenverarbeitung nur solche Arbeitnehmer oder sonstigen Personen ein, die unter Hinweis auf die ordnungswidrigkeits- und strafrechtlichen Folgen zur Vertraulichkeit bzw. Wahrung des Datengeheimnisses verpflichtet worden sind.

(2) Der Auftragnehmer wird durch technische und organisatorische Maßnahmen darauf hinwirken, dass die Arbeitnehmer oder sonstigen Personen, die Zugang zu personenbezogenen Daten aus dem Geschäftsbereich des Auftraggebers haben, diese nur im Rahmen der vertraglichen Vorgaben verarbeiten, es sei denn, sie sind gesetzlich zu einer anderweitigen Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen mit, sobald er von vor der beabsichtigten oder erfolgten Vornahme einer solchen Verarbeitung Kenntnis erlangt, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(3) Der Auftragnehmer benennt einen Verantwortlichen, der seine Tätigkeit gemäß Art. 38 und 39 EU-DSGVO ausübt. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme im Anhang 4 mitgeteilt. Ein Wechsel des Datenschutzbeauftragten oder des Verantwortlichen wird dem Auftraggeber unverzüglich mitgeteilt.

(4) Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der EU-DSGVO bekannt sind. Er verpflichtet sich, auch die für diesen Auftrag relevanten Geheimnisschutzregeln nach § 203 StGB (Berufsgeheimnisträger) zu beachten, die dem Auftraggeber obliegen. Dem Auftragnehmer ist bekannt, dass die im Auftrag ggf. verarbeiteten Patientendaten einer sich aus dem ärztlichen Berufsrecht ergebenden und durch §203 StGB geschützten Schweigepflicht unterliegen, die auch nach dem Ende dieses AV-Vertrages fortbesteht. Der Auftragnehmer wird eine Einhaltung dieser Schweigepflicht gegenüber Dritten sicherstellen und seine von ihm im Rahmen der übertragenen Aufgaben eingesetzten Beschäftigten entsprechend belehren, schulen und verpflichten. Beide Vertragsparteien verpflichten sich, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebs- und Geschäftsgeheimnissen, auch über das Vertragsverhältnis hinaus, vertraulich zu behandeln bzw. Stillschweigen

über die ihnen im Zusammenhang mit dem Auftrag bekannt gewordenen Daten zu wahren.

§ 7 Datensicherheitskonzept

(1) Der Auftragnehmer verpflichtet sich, im Rahmen der Auftragsverarbeitung die technischen und organisatorischen Maßnahmen zu treffen bzw. aufrecht zu erhalten, die im Datensicherheitskonzept festgeschrieben sind. Das zum Zeitpunkt der Unterzeichnung dieses Vertrags aktuelle Datensicherheitskonzept ist als Überblick als Anhang 2 beigefügt.

(2) Dem Auftragnehmer ist es gestattet, das Datensicherheitskonzept durch einseitige Änderungen fortzuschreiben und sodann entsprechende technische und organisatorische Maßnahmen zu ergreifen. Das jeweils aktuelle Datensicherheitskonzept ist dem Auftraggeber mitzuteilen. Fortschreibungen sind insbesondere vorzunehmen wegen Änderungen der gesetzlichen Rahmenbedingungen sowie gerichtlicher oder behördlicher Vorgaben gegenüber dem Auftraggeber, dem Auftragnehmer oder einem anderen Kunden des Auftragnehmers, der dieselbe standardisierte Leistung des Auftragnehmers in Anspruch nimmt, die eine Änderung notwendig machen. Durch Fortschreibungen können vorher im Datensicherheitskonzept enthaltene einzelne Maßnahmen entfallen, ohne dass sie durch artverwandte Maßnahmen ersetzt werden müssten. Eine geplante Fortschreibung des Datensicherheitskonzepts durch den Auftragnehmer ist unzulässig, wenn dadurch das Schutzniveau der Maßnahmen des aktuellen Datensicherheitskonzepts unmittelbar vor der geplanten Fortschreibung in Summe abgesenkt würde.

(3) Die Befugnis des Auftragnehmers zur Fortschreibung des Datensicherheitskonzepts berührt nicht die alleinige Verantwortlichkeit des Auftraggebers zur Beurteilung der im Datensicherheitskonzept festgelegten Maßnahmen und des durch diese gewährleisteten Schutzniveaus. Eine Beratung des Auftraggebers zur Tauglichkeit und Erforderlichkeit von Maßnahmen im Sinne von Art. 32 Abs. 1 EU-DSGVO wird vom Auftragnehmer nur insofern geschuldet, als dies Bestandteil eines Angebots des Auftragnehmers ist. Änderungswünsche des Auftraggebers hinsichtlich des Datensicherheitskonzepts und der daraufhin vom Auftragnehmer zu ergreifenden Maßnahmen wird der Auftragnehmer nicht unbillig ablehnen, wenn der Auftraggeber

die Übernahme der durch die Realisierung seiner Änderungswünsche entstehenden Kosten zugesagt hat.

§ 8 Beauftragung von Subunternehmern

(1) Dem Auftragnehmer ist es im Allgemeinen gestattet, seine Leistungen durch Subunternehmer erbringen zu lassen.

(2) Für die in Anhang 3 dieser Vereinbarung aufgeführten Subunternehmer hat der Auftraggeber seine Zustimmung erteilt.

(3) Über jede beabsichtigte Hinzuziehung, Änderung in Bezug auf die Hinzuziehung oder die Ersetzung solcher Subunternehmer, d.h. anderer Auftragsverarbeiter, wird der Auftragnehmer den Auftraggeber rechtzeitig informieren, so dass dieser die Möglichkeit erhält, binnen zehn Werktagen ab Zugang der Information Einspruch zu erheben. Sowohl die Information, als auch der Einspruch bedürfen zu ihrer Wirksamkeit mindestens der Textform. Der Einspruch bedarf darüber hinaus der Angabe eines Grundes.

(4) Geht der Einspruch dem Auftragnehmer fristgerecht zu und ist ein Grund angegeben, wird der Auftragnehmer angemessene Anstrengungen unternehmen, um dem Auftraggeber eine Anpassung der jeweils betroffenen Leistungen zur Verfügung zu stellen oder um eine wirtschaftlich zumutbare Anpassung der Nutzung der jeweils betroffenen Leistungen vorzuschlagen, um eine Verarbeitung personenbezogener Daten durch den beanstandeten Subunternehmer zu vermeiden, ohne den Auftraggeber übermäßig zu belasten. Falls der Auftragnehmer eine derartige Anpassung nicht innerhalb eines angemessenen Zeitraums von maximal dreißig Tagen vornehmen kann, kann der Auftraggeber diesen Vertrag schriftlich oder in einem dokumentierten elektronischen Format gegenüber dem Auftragnehmer kündigen. Andernfalls gilt die Genehmigung des Auftraggebers als erteilt.

(5) Verarbeitungen, die durch den beabsichtigten Einsatz eines Subunternehmers ausgeführt werden sollen, darf der Auftragnehmer für die Dauer der Einspruchsfrist aufschieben, um die Entscheidung des Auftraggebers abzuwarten.

(6) Der Auftragnehmer ist verpflichtet, die in Art. 28 Abs. 4 EU-DSGVO genannten Voraussetzungen einzuhalten.

(7) Dem Auftragnehmer ist bekannt, dass die im Auftrag ggf. verarbeiteten Patientendaten einer sich aus dem ärztlichen Berufsrecht ergebenden und durch §203 StGB geschützten Schweigepflicht unterliegen, die auch nach dem Ende dieses AV-Vertrages fortbesteht. Der Auftragnehmer wird seine von ihm im Rahmen der

übertragenen Aufgaben eingesetzten Subunternehmer (gemäß Anhang 3) entsprechend belehren, schulen und verpflichten.

§ 9 Erfüllung der Rechte betroffener Personen

(1) Ist der Auftraggeber gegenüber einer betroffenen Person aufgrund geltendem Datenschutzrecht verpflichtet, wird der Auftragnehmer den Auftraggeber bei der Erfüllung seiner Verpflichtungen unterstützen, sofern und soweit dazu in tatsächlicher Hinsicht Handlungen des Auftragnehmers unerlässlich sind und soweit derartige Mitwirkungen dem Auftragnehmer zumutbar sind.

(2) Wendet sich eine betroffene Person mit Anfragen oder Ansprüchen unmittelbar an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen. Sofern und soweit der Auftragnehmer im Zusammenhang mit der Auftragsverarbeitung gegenüber der betroffenen Person kraft Gesetzes verpflichtet ist, wird der Auftragnehmer den Auftraggeber über die Erfüllung berechtigter Ansprüche der betroffenen Person informieren.

§ 10 Informationspflichten des Auftragnehmers

(1) Über Maßnahmen der datenschutzrechtlichen Aufsichtsbehörde sowie über Ermittlungsmaßnahmen von Strafverfolgungsbehörden beim Auftragnehmer bezüglich des Verdachts der Begehung datenschutzrechtlicher Straftaten wird der Auftragnehmer den Auftraggeber informieren, sofern von den Maßnahmen die Verarbeitung personenbezogener Daten aus dem Geschäftsbereich des Auftraggebers betroffen sind.

(2) Wenn dem Auftragnehmer eine Verletzung des Schutzes personenbezogener Daten bekannt wird, informiert er den Auftraggeber von dieser unverzüglich, sofern die von der Verletzung des Schutzes betroffenen Daten aus dem Geschäftsbereich des Auftraggebers stammen. Dabei hat der Auftragnehmer alles mitzuteilen, was ihm positiv bekannt ist und nachlaufende Mitteilungen zu machen, sobald Weiteres bekannt wird.

(3) Hat der Auftraggeber eine Datenschutz-Folgenabschätzung und ggf. eine vorherige Konsultation durchzuführen, wird der Auftragnehmer den Auftraggeber bei der Erfüllung seiner Verpflichtungen unterstützen, sofern und soweit dazu in tatsächlicher Hinsicht Handlungen des Auftragnehmers unerlässlich sind und soweit derartige

Mitwirkungen dem Auftragnehmer zumutbar sind oder dies Gegenstand eines Vertrags mit dem Auftragnehmer ist.

§ 11 Prüf-, Zutritts- und Auskunftsrechte des Auftraggebers

(1) Der Auftraggeber darf beim Auftragnehmer Informationen zum Nachweis der Einhaltung der in Art. 28 EU-DSGVO niedergelegten Pflichten einholen und zu diesem Zwecke Überprüfungen beim Auftragnehmer durchführen.

(2) Derartige Überprüfungen werden regelmäßig durch Einholung einer Selbstauskunft vom Auftragnehmer durchgeführt. Der Auftragnehmer ist berechtigt, die Abgabe einer Selbstauskunft durch die Überlassung von Kopien von Testaten oder Zertifizierungen durch Dritte zu ergänzen oder zu ersetzen, sofern diese nicht älter als ein Jahr sind.

(3) Für den Fall sachlich begründeter Zweifel an der Richtigkeit oder Vollständigkeit der Aussagen in einer Selbstauskunft oder in Testaten oder Zertifizierungen sowie für den Fall des Vorliegens eines wichtigen Grundes (z.B. Nachprüfung im zeitlich unmittelbaren Anschluss an eine Mitteilung des Auftragnehmers gem. Ziff. Informationspflichten) verpflichtet sich der Auftragnehmer, die Durchführung einer Kontrolle vor Ort zu dulden. Der Auftragnehmer räumt dem Auftraggeber für diese Fälle und zu diesem Zweck das Recht ein, sich nach rechtzeitiger Anmeldung im Rahmen üblicher Bürozeiten in den Betriebsräumen des Auftragnehmers ohne wesentliche Störung des Betriebsablaufes des Auftragnehmers von der Einhaltung der vertraglichen Vorgaben sowie der Pflichten aus Art. 28 EU-DSGVO zu überzeugen. Zu diesem Zweck erforderliche Auskünfte darf der Auftraggeber nur bei der Geschäftsleitung des Auftragnehmers einholen und dies nur in einem Umfang, der dem Auftragnehmer zumutbar ist.

(4) Die Prüf-, Zutritts- und Auskunftsrechte nach dieser Ziffer kann der Auftraggeber nur selbst, durch eigene Arbeitnehmer oder durch von ihm auf eigene Kosten zu beauftragende externe Prüfer wahrnehmen. Die konkrete Person ist vorab namentlich anzukündigen. Als externe Prüfer kommen nur von Berufs wegen zur Verschwiegenheit Verpflichtete in Betracht und dies auch nur dann, wenn der Auftraggeber dem Auftragnehmer vor Beginn der Prüfung nachweist, dass er mit dem jeweiligen Berufsträger die nicht ohne Mitwirkung des Auftragnehmers wieder

aufhebbare Einbeziehung des Auftragnehmers in den Schutzbereich der berufsmäßigen Verschwiegenheitspflichten vereinbart hat.

(5) Der Auftraggeber hat die von ihm vorgenommene Kontrolle vor Ort und ihre Ergebnisse zeitnah zu dokumentieren und die Dokumentation unverzüglich nach Erstellung dem Auftragnehmer vollständig in Kopie zu überlassen.

§ 12 Beendigung des Auftrags

(1) Endet dieser Vertrag – gleich aus welchem Rechtsgrund – wird der Auftragnehmer alle noch in seinen Besitz befindlichen Daten aus dem Geschäftsbereich des Auftraggebers der Löschung bzw. Vernichtung zuführen, sofern und soweit nicht der Auftraggeber bei Beendigung des Vertrages oder spätestens unverzüglich danach den Auftragnehmer anweist, diese Daten zurückzugeben.

(2) Der Auftragnehmer ist berechtigt, sowohl eine solche Löschung bzw. Vernichtung als auch eine Rückgabe ausnahmsweise zu unterlassen, sofern und soweit rechtliche Anforderungen an den Auftragnehmer entgegenstehen. Der Auftragnehmer wird solche rechtlichen Anforderungen dem Auftraggeber mitteilen, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(3) Solange nicht alle personenbezogenen Daten, die im Auftrag des Auftraggebers verarbeitet wurden und nach Wegfall des Hauptvertrags noch im Besitz des Auftragnehmers waren, vom Auftragnehmer gelöscht bzw. vernichtet oder an den Auftraggeber zurückgegeben wurden, gilt dieser Vertrag als fortbestehend hinaus. Ist vorgenannte Bedingung entfallen, endet dieser Vertrag, ohne dass es einer gesonderten Erklärung von einer der Parteien bedarf.

§ 13 Umfang des Vertrages, Rangfolge von Dokumenten

(1) Als Bestandteile dieses Vertrages gelten die folgenden Anhänge:

- Anhang 1 – Ergänzende Festlegungen zum Auftrag
- Anhang 2 – Datensicherheitskonzept / Kurzbeschreibung technische und organisatorische Maßnahmen
- Anhang 3 – Subunternehmer
- Anhang 4 – Verantwortlicher des Auftragnehmers für die Verarbeitung personenbezogener Daten

(2) Wird der Anhang 1 als Mustervorlage verwendet und mehrfach ausgefüllt, z. B. bei der Beauftragung verschiedener Leistungen mit kategorisch unterschiedlichen Daten, gelten alle ausgefüllten Exemplare des Anhang 1 als Bestandteile dieses Vertrages. Das

Datensicherheitskonzept ist im Falle von Fortschreibungen in der jeweils beim Auftragnehmer vorhandenen, aktuellen Fassung Bestandteil dieses Vertrages.

(3) Die Vereinbarungen dieses Vertrages genießen Vorrang vor allen anderen Vereinbarungen der Parteien.

(4) Gerichtsstand ist Stuttgart.

Für den Auftraggeber:	**Für den Auftragnehmer:** Praxis der Zukunft GmbH
_____	**Ort, Datum:**
Ort, Datum:	Stuttgart, den 03.02.2021
_____	**Geschäftsführerin:** Sigrid Borst
Name in Druckbuchstaben:	
_____	
Funktion:	**Unterschrift:** Sigrid Borst
_____	
Unterschrift:_____	

Anhang 1: Ergänzende Festlegungen zum Auftrag

Gegenstand des Auftrages	Der Gegenstand des Auftrages ergibt sich grundsätzlich aus dem zugrunde liegenden Auftrag / Angebot.
Art und Zweck der Verarbeitung	Als Arten der Verarbeitung personenbezogener Daten durch den Auftragnehmer sind – sofern im zugrunde liegenden Auftrag nicht anders oder näher bezeichnet – insbesondere: • Die Durchführung von Analyse- und Optimierungsmaßnahmen im Bereich der ärztlichen Abrechnung • Beratungsmaßnahmen im Bereich ärztlicher Abrechnung • Anwenderunterstützung und Hilfestellung Die Verarbeitung findet per Telefon, E-Mail, Fernzugriff oder vor-Ort statt und in den Räumlichkeiten des Auftragnehmers. Der Zweck der Verarbeitung ist • die Optimierung der ärztlichen Abrechnung • die Beratung zur Nutzung wirtschaftlicher Potenziale,
Kategorien betroffener Personen	Mitarbeiter, Inhaber sowie Patienten des Auftraggebers
Art der personenbezogenen Daten	Im Rahmen der Leistungserbringung ist ein Kontakt mit allen Arten personenbezogener Daten des Auftraggebers möglich und kann nicht sicher ausgeschlossen werden. Hierzu gehören unter anderem: • Namen • Daten über Geburt und Familienstand • private und geschäftliche Kontaktdaten (z. B. Post-Adressen, E-Mail-Adressen, Telefonnummern) • Versicherungsdaten • Protokolldaten • Patientendaten • medizinischen Daten (z. B. Bilddaten, Analyseergebnisse, Diagnosen, Befunde) • Leistungsdaten (z. B. Daten zu Maßnahmen, Therapien und Medikationen)

	• Abrechnungs- und Kostendaten • Namen, Telefonnummern, Geburtsdatum, Funktion, E-Mailadresse von Mitarbeitern des Auftraggebers zur Nutzung der vom Auftragnehmer bereitgestellter Systeme.
Liste der weiteren Weisungsempfänger des Auftragnehmers	Alle Mitarbeiter des Auftragnehmers in den Bereichen Beratung, Datenanalyse, Sekretariat, Buchhaltung.

Anhang 2: Übersicht Datensicherheitskonzept: Technische und organisatorische Maßnahmen

Der Auftragnehmer legt großen Wert auf einen optimalen Schutz von personenbezogenen Daten. Daher gibt es umfangreiche technische und organisatorische Maßnahmen um ein hohes Schutzniveau zu erreichen. Diese Maßnahmen werden in diesem Dokument im Überblick beschrieben.

(1) Allgemeines

Wir orientieren uns bei den technischen und organisatorischen Maßnahmen an gängigen Standards, wie dem BSI-Grundschutzstandard. Das hohe Schutzniveau unserer Maßnahmen wird regelmäßig überprüft und an den jeweils aktuellen Stand der Technik angepasst. Mitarbeiter werden im Umgang mit schützenswerten Daten regelmäßig geschult und auf die Vertraulichkeit verpflichtet.
Der Umgang mit Daten und Datenverarbeitungsanlagen ist schriftlich geregelt (Datenschutzrichtlinien, Arbeitsanweisungen, Verfahrensbeschreibungen) und wird regelmäßig überprüft.

(2) Vertraulichkeit (Art. 32 Abs. 1 lit. b EU-DSGVO)

Zutrittskontrolle

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Der Auftragnehmer stellt dies unter anderem durch folgende Maßnahmen sicher:

- Schließsystem
- Schlüsselregelungen
- Protokollierung der Besucher
- Regelungen für Unternehmensfremde

Zugangskontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.
Der Auftragnehmer stellt dies unter anderem durch folgende Maßnahmen sicher:

- Konzeption und Implementierung eines Berechtigungskonzeptes für Endgeräte und IT-Systeme
- Authentifikation mit Benutzername und Passwort, wo nötig, 2-Faktor-Authentifizierung
- Automatische Sicherstellung sicherer Passwörter (Passwortrichtlinie)
- Festlegung und regelmäßige Kontrolle der Zugangsbefugnisse
- Verschlüsselung von mobilen Endgeräten und mobilen Datenträgern
- Einsatz von zentral verwalteter Anti-Viren-Software

- Einsatz von Hardware-Firewalls
- Einsatz von VPN-Technologie
- Einsatz von zertifizierter Fernwartungssoftware TeamViewer / AnyDesk
- Überwachung von Zugangsversuchen
- Regelungen für Unternehmensfremde

Zugriffskontrolle

Es ist zu 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.
Der Auftragnehmer stellt dies unter anderem durch folgende Maßnahmen sicher:

- Berechtigungskonzept für Applikationen
- Verwaltung der Rechte durch den Systemadministrator
- Anzahl der Zugriffsmöglichkeiten auf das „Notwendigste“ reduziert
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Sichere Aufbewahrung von Datenträgern, Verschlüsselung derselben
- physische Löschung von Datenträgern vor Wiederverwendung
- ordnungsgemäße Vernichtung von Datenträgern und Papierunterlagen (DIN 66399)
- Einsatz von Aktenvernichtern bzw. zertifizierten Dienstleistern
- Schriftliche Regelung zum Umgang mit digitalen Speichermedien
- Funktionsbegrenzungen (zeitlich/funktionell)

Trennungskontrolle

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Der Auftragnehmer stellt dies unter anderem durch folgende Maßnahmen sicher:

- Bei pseudonymisierten Daten (Art. 32 Abs. 1 lit. a EU-DSGVO; Art. 25 Abs. 1 EUDSGVO): Trennung der Zuordnungsdatei und der Daten
- Getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Regelmäßige Prüfung der bestimmungsgemäßen Nutzung der Daten und IT-Systeme
- Trennung von Produktiv- und Testsystemen

(3) Integrität (Art. 32 Abs. 1 lit. b EU-DSGVO)

Weitergabekontrolle

Es ist zu 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 welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Der Auftragnehmer stellt dies unter anderem durch folgende Maßnahmen sicher:

- Einsatz geeigneter Verschlüsselung
- Einsatz von VPN-Technologie
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- Maßnahmen zur Verhinderung von unkontrollierten Informationsabflüssen

Eingabekontrolle

Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Der Auftragnehmer stellt dies unter anderem durch folgende Maßnahmen sicher:

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind

(4) Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b EU-DSGVO), sowie Verfügbarkeitskontrolle und rasche Widerherstellbarkeit (Art. 32 Abs. 1 lit. c EU-DSGVO)

Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und System und Dienste ausreichend belastbar sind. Der Auftragnehmer stellt dies unter anderem durch folgende Maßnahmen bei sich und seinen IT-Dienstleistern sicher:

- Feuerlöschgeräte für die IT-Infrastruktur
- Konzept zur Datensicherung und Wiederherstellung
- Vorbereitete Notfallplanung
- Testen von Datenwiederherstellung
- Einsatz von redundanten IT-Systemen

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

Incident-Response-Management

Der Auftragnehmer stellt dies unter anderem durch folgende Maßnahmen sicher:

- Strukturierte Bewertung und Priorisierung gemeldeter bzw. erkannter technischer Störungen und Sicherheitsvorfälle
- Festgelegte interne und externe Kommunikations- und Eskalationsprozesse
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 EU-DSGVO)

Der Auftragnehmer stellt dies unter anderem durch folgende Maßnahmen sicher:

- Systeme und Anwendungen werden vor der Verwendung sicher konfiguriert und voreingestellt („privacy by default“).
- Produkte werden nach dem Prinzip „privacy by design“ entwickelt
- Standardeinstellungen der Produkte anderer Hersteller werden vor der ersten Verwendung überprüft und sicher angepasst

Auftragskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.
Der Auftragnehmer stellt dies unter anderem durch folgende Maßnahmen sicher:

- Auswahl der Auftragnehmer unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- Schriftliche Weisungen an die Auftragnehmer

- Vereinbart wirksame Kontrollrechte gegenüber den Auftragnehmern
- Prüfung und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Regelmäßige Überprüfung des Auftragnehmers und seiner Tätigkeiten

Anhang 3: Subunternehmer

Für die nachfolgend aufgeführten Subunternehmer hat der Auftraggeber gemäß „§ 7 Beauftragung von Subunternehmern“ seine Zustimmung erteilt:

Beratungsleistungen bei Bedarf:
medmanager UG
Dipl.-Kfm. Joachim Deuser
Schillerstr. 10A
12207 Berlin

Tel. 030-698158-61
Fax: 030-698158-67

Mail: joachim.deuser@medmanager.de

Anhang 4: Verantwortlicher für die Verarbeitung personenbezogener Daten des Auftragnehmers

Name	Sigrid Borst
Postanschrift	Vaihinger Straße 95, 70567 Stuttgart
Kontaktdaten: (E-Mail, Telefon, ggf. Telefax)	Telefon: 0178/8127359 E-Mail:kontakt@hzv-abrechnung.de