e-health.software

ist ein Angebot der Haedge Consulting GmbH
- im Folgenden Auftragnehmerin genannt -

Vereinbarung zur Auftragsverarbeitung

§ 1 Gegenstand und Dauer der Auftragsverarbeitung

(1) Gegenstand

Die Auftragnehmerin übernimmt für Auftraggebende abhängig von den abonnierten Standardsoftwarelösungen bzw. für sie individuell erstellte Software und beauftragte Serviceleistungen

- den fachlichen und technischen Support
- den Versand von Abrechnungsdaten an Datenannahmestellen der Kostenträger
- die Prüfung und gegebenenfalls Weiterleitung von Abrechnungsunterlagen
- die Online-Datensicherung
- die sichere Verwahrung von Zugangsdaten

(2) Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der jeweils zugrunde liegenden Leistungsvereinbarung und ist an diese gekoppelt.

§ 2 Auftragsinhalt

Der Umfang der Tätigkeiten die Auftragnehmerin richtet sich nach den Anforderungen der Auftraggebenden und beinhaltet

- fachlichen und technischen Support für von der Auftragnehmerin bereitgestellte Softwarelösungen der Auftraggebenden nach Art und Umfang der von der Auftraggebenden beschriebenen Problemlage. In Fällen, in denen eine Problemlösung nicht rein telefonisch erfolgen kann, schaltet sich die Auftragnehmerin über das Internet mit Hilfe einer Remote-Support-Software auf das betroffene Endgerät der Auftraggebenden auf, um die angeforderten Tätigkeiten durchzuführen.

  Die Autorisierung der Aufschaltung erfolgt durch die Auftraggebenden mit Hilfe einer telefonisch übermittelten Sitzungsnummer. Die Auftraggebenden haben die Möglichkeit, die Sitzung zu überwachen und sie jederzeit zu beenden. Änderungen an Nutzdaten werden im Regelfall durch die Auftraggebenden ausgeführt. In Einzelfällen können die Auftraggebenden Mitarbeitende der Auftragnehmerin autorisieren, solche Änderungen vorzunehmen. Alle mit Support-Aufgaben betrauten Mitarbeitenden der Auftragnehmerin sind vertraglich zur Wahrung der Vertraulichkeitsverpflichtung gem Art. 28 Abs. 3 S. 2 lit. b) i.V.m. Art. 29 DSGVO verpflichtet.
- den Versand von Abrechnungsdaten an die Datenannahmestellen der Kostenträger nach dem Ergebnis des Sendevorgangs. Die von Auftraggebenden mit dem Abrechnungsprogramm für gesetzlich versicherte Betreute erstellten Rechnungen werden asymmetrisch verschlüsselt an das ServiceCenter der Auftragnehmerin übertragen. Die Weiterleitung der Abrechnungsdaten an die Datenannahmestellen erfolgt vollautomatisch in einem geschlossenen System: die übertragenen Rechnungen liegen während der datentechnischen Aufbereitung temporär und ausschließlich im Arbeitsspeicher entschlüsselt vor und werden im Anschluss, wiederum verschlüsselt, unverzüglich weitergeleitet. Sobald der Rechnungseingang bei der Datenannahmestelle erfolgt ist, werden die personenbezogenen Daten im ServiceCenter der Auftragnehmerin nach Ablauf der jeweils gültigen Reklamationsfrist gelöscht. Werden Abrech-

nungsdaten abgewiesen, erfolgt zusätzlich der Versand einer entsprechenden Abweisungsmitteilung an die Auftraggebenden. Die Abweisungsmitteilung enthält keine personenbezogenen Daten.

- die Prüfung von Abrechnungsunterlagen zur Vorbereitung der Erfassung bzw. des Rechnungsankaufes auf Vollständigkeit und Plausibilität der eingegangenen Dokumente zur Rechnungserstellung. Die Auftraggebenden erfassen ihre Abrechnungsdaten mit der von der Auftragnehmerin bereitgestellten Software und übermitteln die Daten, sowie gegebenenfalls anfallende Papierunterlagen an das ServiceCenter der Auftragnehmerin. Im Fall der Buchung des Service Komplettabrechnung übersenden die Auftraggebenden die Abrechnungsunterlagen zur weiteren Bearbeitung an das ServiceCenter der Auftragnehmerin. Dort erfolgt in beiden Fällen eine Prüfung auf Plausibilität und Vollständigkeit. Im Fall des Services Komplettabrechnung kann anschließend die Weiterleitung der Abrechnungsunterlagen an einen Kooperationspartner zur Erfassung erfolgen. Kann für einen Abrechnungsfall keine Freigabe erfolgen, werden Rückläuferprozesse mit dem Ziel initiiert, vollständige und plausible Abrechnungsunterlagen zu erwirken. Liegen diese vor, so erfolgen die Freigabe der Abrechnung und die Weiterleitung der Abrechnungsunterlagen gegebenenfalls an einen Kooperationspartner zum Rechnungs-Ankauf. Mit solchen Kooperationspartnern besteht jeweils eine Vereinbarung zur Auftragsverarbeitung, die auf Verlangen bereitgestellt wird. Sobald die Bearbeitung einer Rechnung bei dem Kooperationspartner für den Rechnungs-Ankauf abgeschlossen ist, werden die entsprechenden Patientendaten im ServiceCenter der Auftragnehmerin gelöscht.
- Bei einer Online-Datensicherung fällt keine Verarbeitung personenbezogener Daten durch die Auftragnehmerin an. Die lokal von der Auftraggebenden in der Software vorgehaltenen Daten werden verschlüsselt und auf einen vom ServiceCenter der Auftragnehmerin verwalteten Server hochgeladen. Auf diese Weise können Auftraggebende im Schadensfall ihre Daten wieder in ihr lokales System zurückspielen. Über den Schlüssel verfügen nur die Auftraggebenden, so dass weder das ServiceCenter der Auftragnehmerin noch Dritte Daten lesen können.
- die sichere Verwahrung von Zugangsdaten. Alle mit der Verwahrung von Zugangsdaten betrauten Mitarbeitenden der Auftragnehmerin sind vertraglich zur Wahrung der Vertraulichkeitsverpflichtung gemäß Art. 28 Abs. 3 S. 2 lit. b) i.V.m. Art. 29 DSGVO verpflichtet.

Die Erbringung der Auftragsverarbeitung findet aus-schließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

§ 3 Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten können folgende Datenarten/-kategorien sein:

- Adressdaten
- Vertragsstammdaten
- Kontakt-/Kommunikationsdaten
- Geburtsdatum, Geschlecht
- Gesundheitsdaten, insb. nach Art. 4 Nr. 15 DSGVO
- Sozialdaten gem. § 67 Abs. 1 SGB X
- Daten, die für die Abrechnung von Leistungen mit den Kostenträger erforderlich sind
- Versichertendaten
- kooperierende Leistungserbringer
- Rechnungsdaten
- Zahlungsdaten
- Kundenhistorie
- Sonstige personenbezogene Daten

§ 4 Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen können sein:

- Kundinnen
- Interessentinnen
- Beschäftigte
- Kooperationspartner
- Betreute/Patienten (gesetzlich und privat Versicherte sind betroffene Personen im Sinne des Art.4 Nr. 1 DSGVO)

§ 5 Technisch-organisatorische Maßnahmen

(1) Die Auftragnehmerin stellt Auftraggebenden die Dokumentation der technischen und organisatorischen Maßnahmen auf Anforderung zur Verfügung. Die dokumentierten Maßnahmen werden Grundlage der Auftragsverarbeitung. Soweit sich durch die Prüfung/ein Audit von Auftraggebenden einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Die Auftragnehmerin 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.

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

§ 6 Berichtigung, Einschränkung und Löschung von Daten

(1) Die Auftragnehmerin darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung der Auftraggebenden berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an die Auftragnehmerin wendet, wird die Auftragnehmerin dieses Ersuchen unverzüglich an die Auftraggeberin weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht-auf-Vergessen-werden, Berichtigung, Daten-Portabilität und Auskunft nach dokumentierter Weisung der Auftraggebenden unmittelbar durch die Auftragnehmerin sicherzustellen.

§ 7 Qualitätssicherung und sonstige Pflichten der Auftragnehmerin

Sobald die Auftragnehmerin auf Grundlage von § 38 BDSG verpflichtet ist, zusätzlich zu der Einhaltung der Regelungen dieses Auftrags, gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO einzuhalten, gewährleistet sie insbesondere die Einhaltung folgender Vorgaben:

- Schriftliche Bestellung eines Datenschutz-Beauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt. Dessen Kontaktdaten sind in der Datenschutzerklärung auf https://www.e-health.software leicht zugänglich hinterlegt.

Darüber hinaus sichert sie die Qualität der Auftragsverarbeitung wie folgt:

- Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO: die Auftragnehmerin setzt bei der Durchführung der Arbeit mit besonderem Schutz unterliegenden Personendaten nur Beschäftigte ein, die auf die Vertraulichkeit und für die Fälle der Einbeziehung des § 203 StGB in das Vertragsverhältnis auf die Schweigepflicht nach § 203 StGB verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Die Auftragnehmerin und jede der Auftragnehmerin unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung Auftraggebenden verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
- Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO.
- Zusammenarbeit mit Auftraggebenden und auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben.
- Unverzügliche Information von Auftraggebenden 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 bei der Auftragnehmerin ermittelt.

- Unterstützung von Auftraggebenden soweit sie ihrerseits 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.
- Regelmäßige Kontrolle der internen Prozesse sowie der technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in ihrem 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 Auftraggebenden im Rahmen ihrer Kontrollbefugnisse nach § 10 dieses Vertrages.

§ 8 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 die Auftragnehmerin 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. Die Auftragnehmerin ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten der Auftraggebenden auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) die Auftragnehmerin darf Unterauftragnehmerin (weitere Auftragsverarbeiter) nur nach vorheriger, ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung der Auftraggebenden beauftragen. Die Auslagerung auf Unterauftragnehmer oder der Wechsel bestehender Unterauftragnehmer sind zulässig, soweit:

die Auftragnehmerin eine solche Auslagerung auf Unterauftragnehmer der Auftraggebenden eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und

Auftraggebende nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber der Auftragnehmerin schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 4 DSGVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten der Auftraggebenden an Unterauftragnehmer und deren erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Eine weitere Auslagerung durch Unterauftragnehmer bedarf der ausdrücklichen schriftlichen Zustimmung der Auftraggebenden sowie der Hauptauftragnehmer. Sämtliche vertraglichen Regelungen in der Vertragskette sind auch weiteren Unterauftragnehmern aufzuerlegen.

(5) Dem Einsatz von Mitarbeitenden der Auftragnehmerin in mobiler Arbeit oder im Home-Office stimmen die Auftraggebenden zu. Die Auftragnehmerin stellt in solchen Fällen sicher, dass die jeweils gültigen Regelungen zu Datenschutz und -sicherheit auch an diesen Arbeitsplätzen eingehalten werden.

§ 9 Kontrollrechte und Pflichten der Auftraggeberin

(1) Auftraggebende haben das Recht, im Benehmen mit der Auftragnehmerin Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen und sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch die Auftragnehmerin in dessen Geschäftsbetrieb zu überzeugen.

(2) Die Auftragnehmerin stellt sicher, dass sich Auftraggebende von der Einhaltung der Pflichten der Auftragnehmerin nach Art. 28 DSGVO überzeugen kann. Die Auftragnehmerin verpflichtet sich, Auftraggebenden 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 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 oder DIN-ISO 27001)

(4) Für die Ermöglichung von Kontrollen durch Auftraggebende kann die Auftragnehmerin einen Vergütungsanspruch geltend machen. Dieser darf die tatsächlich entstandenen Kosten nicht überschreiten.

(5) Auftraggebende haben ihren Pflichten gegenüber Betroffenen gemäß Art. 13 DSGVO nachzukommen und Betroffenen mitzuteilen, dass die Auftragnehmerin und die einbezogenen Unterauftragnehmer in die Verarbeitung ihrer personenbezogenen Daten involviert sind. Insofern verpflichten sich Auftraggebende zur Einhaltung und Umsetzung ihrer Pflichten nach der EU-DSGVO. Ferner sind Auftraggebende verpflichtet, sofern sie Berufsgeheimnistragende sind, ggf. eine Schweigepflichtentbindungserklärung gemäß Art. 9 Abs. 2 lit. a DSGVO, von den Betroffenen einzuholen. Diese haben sie der Auftragnehmerin auf Anfrage (Stichprobenprüfung) zur Verfügung zu stellen. Etwas anderes gilt dann, wenn sie die Auftragnehmerin wirksam nach § 203 Abs. 4 S. 1 StGB verpflichtet hat.

§ 10 Mitteilung bei Verstößen der Auftragnehmerin

(1) Die Auftragnehmerin unterstützt Auftraggebende bei der Einhaltung der in den Art. 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 Auftraggebende zu melden.
- die Verpflichtung, Auftraggebende im Rahmen ihrer Informationspflicht gegenüber Betroffenen zu unterstützen und ihnen in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen.
- die Unterstützung Auftraggebender für deren Datenschutz-Folgenabschätzung.
- die Unterstützung Auftraggebender im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

(2) Für Unterstützungsleistungen, die nicht Abonnement enthalten oder nicht auf ein Fehlverhalten der Auftragnehmerin zurückzuführen sind, kann die Auftragnehmerin eine Vergütung beanspruchen.

§ 11 Weisungsbefugnis der Auftraggeberin

(1) Die Auftragnehmerin verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung der Auftraggebenden gemäß Art. 28 Abs. 3 lit. a) DSGVO, es sei denn, dass sie nach dem Recht der Europäischen Union oder eines Mitgliedstaates zur Verarbeitung verpflichtet ist. In einem solchen Fall teilt die Auftragnehmerin den Auftraggebenden diese

rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht aus wichtigen Gründen des öffentlichen Interesses verbietet.

(2) Mündliche Weisungen bestätigen Auftraggebende unverzüglich in Schriftform.

(3) Die Auftragnehmerin ist gemäß Art. 28 Abs. 3 S. 2 lit. h) DSGVO verpflichtet, Auftraggebende unverzüglich zu informieren, wenn sie der Meinung ist, eine Weisung verstoße gegen diese Verordnung oder gegen andere Datenschutzbestimmungen der Europäischen Union oder der Mitgliedstaaten. Die Auftragnehmerin ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch Auftraggebende bestätigt oder geändert wird.

§ 12 Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate Daten werden ohne Wissen von Auftraggebenden 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.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch Auftraggebende – spätestens mit Beendigung der Leistungsvereinbarung – hat die Auftragnehmerin sämtliche in ihren Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, Auftraggebenden auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Ausgenommen von dieser Regel sind Daten, die die Auftragnehmerin zur Wahrung der gesetzlichen Aufbewahrungsfristen nicht löschen darf.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch die Auftragnehmerin entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Sie kann sie zu ihrer Entlastung bei Vertragsende Auftraggebenden übergeben.

- Ende der Vereinbarung zur Auftragsverarbeitung -

Die Vereinbarung wird Auftraggebenden in Textform übermittelt und ist ohne Unterschrift gültig.

Anlage Technisch-organisatorische Maßnahmen

Die Dokumentation der technischen und organisatorischen Maßnahmen nach Art. 32 Abs. 1 DSGVO ist Bestandteil dieses Auftrages und kann bei der Auftragnehmerin in aktueller Form angefordert werden. Bei Abschluss dieser Vereinbarung wurden die technischen und organisatorischen Maßnahmen durch die Auftraggeberin oder durch eine von ihr bevollmächtigte Person kontrolliert und für ausreichend befunden. Diese zum Datenschutz getroffenen Maßnahmen unterliegen dem technischen Fortschritt und werden somit fortlaufend aktualisiert.