Anlage B

zur Dienstleistungsvereinbarung DZH.finance

Diese Vereinbarung regelt die Maßnahmen zum Schutz von personenbezogenen Daten gem. Art. 4 Nr. 1 EU-DSGVO, Gesundheitsdaten gem. Art. 4 Nr. 15 EU-DSGVO und Sozialdaten im Sinne des § 67 Abs. 2 SGB X bei der Datenverarbeitung im Auftrag unter Berücksichtigung der Art. 28, 29 EUDSGVO und der § 80 SGB X sowie § 29 KDG, § 29 KDR-OG und §30 DSG-EKD.

1. Gegenstand und Dauer des Auftrags

1.1. Gegenstand
- Der Gegenstand des Auftrags ergibt sich aus dem Rahmenvertrag DZH.finance nebst seiner einbezogenen Anlagen, hier verwiesen wird (im Folgenden „Leistungsvereinbarung“).

1.2. Dauer
- Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung und ist an diese gekoppelt.

2. Konkretisierung des Auftragsinhalts

2.1. Art und Zweck der vorgesehenen Verarbeitung von Daten
- Die Finanzdienstleistung des Auftragnehmers beinhaltet die Auszahlung sämtlicher Krankenkassenrechnungen/Betroffenenrechnung einer Periode in einer Summe auf der Basis von Summenabrechnungen zu einem Zeitpunkt, den der Auftraggeber mit dem Auftragnehmer fix vereinbaren kann.
- Zur Konkretisierung der angekauften Forderungen werden die Rechnungsnummern und Vor- und Nachname des Patienten/Versicherten und bei Stellung von Privatrechnungen auch die Adresse des Patienten/Versicherten an den Auftragnehmer übermittelt.
- 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.

2.2. Art der Daten
Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

- Name
- Adressdaten
- Kontaktdaten

2.3. Kategorien betroffener Personen
Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:
- Auftraggeber
- Mitarbeiter des Auftraggebers
- Versicherte/Betroffene (gesetzlich bzw. privat Versicherte - betroffene Personen im Sinne des Art. 1. DSGVO)

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 ein-vernehmlich umzusetzen.

3.2. Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 S. 2 lit. c), Art. 32 EU-DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 EU-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 EU-DSGVO zu berücksichtigen.

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. Berechtigung, Einschränkung und Löschung von Daten

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

4.2. Soweit im Leistungsumfang definiert, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und

Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

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

- Schriftliche Bestellung, soweit nach EU-DSGVO bzw. BDSG erforderlich, eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 EU-DSGVO ausübt.
- Dessen Kontaktdaten werden ggf. dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird ggf. dem Auftraggeber unverzüglich mitgeteilt.
- Dessen jeweils aktuelle Kontaktdaten sind ggf. auf der Website des Auftragnehmers leicht zugänglich hinterlegt.
- Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 EU-DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten 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. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
- Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 EU-DSGVO.
- Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftrag-nehmer ermittelt.
- Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unter-stützen.
- Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
- Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.
- die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
- die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

6. Unterauftragsverhältnisse

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

6.2. Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 EU-DSGVO:

- Firmen der “opta data Unternehmensgruppe“ (https://www.optadata-gruppe.de/unternehmen/unternehmen-der-gruppe)
- Microsoft (E-Mail Kommunikation über Exchange Online) Serverstandort Deutschland

  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, mindestens 14 Tage, vorab schriftlich oder in Textform anzeigt und
  - der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform einen begründeten Einspruch gegen die geplante Auslagerung erhebt und
  - eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 EU-DSGVO zugrunde gelegt wird.

Im Falle eines Einspruchs finden die Parteien eine einvernehmliche Lösung.

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

6.4. Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutz-rechtliche Zulässigkeit durch entsprechende Maßnahmen gem. Art. 44 ff. EU-DSGVO sicher. Gleiches gilt, wenn der Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden soll.

6.5. Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen schriftlichen Zustimmung des Auftrag-

gebers sowie des Hauptauftragnehmers. Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

6.6. Dem Einsatz von Mitarbeitern des Auftragnehmers in Heimarbeit oder im mobilen Arbeiten stimmt der Auftraggeber zu.

7. Kontrollrechte und Pflichten des Auftraggebers

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

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

7.3. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch:

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 EU-DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 EU-DSGVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, Informationssicherheitsbeauftragter , Datenschutzauditoren,- Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz oder ISO 27001).

7.4. Für die Ermöglichung von Kontrollen, die über ein übliches Maß von einmal jährlich hinaus gehen, kann der Auftragnehmer einen Vergütungsanspruch geltend machen. Dieser darf die tatsächlich entstanden Kosten nicht überschreiten.

7.5. Der Auftraggeber hat seinen Pflichten gegenüber dem Betroffenen gemäß Art. 13 EU-DSGVO nachzukommen und dem Betroffenen mitzuteilen, dass der Auftragnehmer und der einbezogene Unterauftragnehmer die Verarbeitung seiner personenbezogenen Daten involviert sind. Insofern verpflichtet sich der Auftraggeber zur Einhaltung und Umsetzung seiner Pflichten nach der EU-DSGVO. Ferner ist der Auftraggeber verpflichtet, bei nicht gesetzlich Versicherten eine Einwilligungserklärung und ggfs. Schweigepflichtentbindungserklärung, gemäß § 203 StGB, Art. 9 Abs. 2 lit. a. und Art. 7 EU-DSGVO des Betroffenen einzuholen. Diese hat er dem Auftragnehmer auf Anfrage (Stichprobenprüfung) zur Verfügung zu stellen.

8. Mitteilung bei Verstößen des Auftragnehmers

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

- die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen.
- die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden.
- die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Behörde

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

9. Weisungsbefugnis des Auftraggebers

9.1. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich in Schriftform.

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

10. Löschung und Rückgabe von personenbezogenen Daten

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

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

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

11. AGB-Klausel

Die DZH ist zu Änderungen der allgemeinen Geschäftsbedingungen berechtigt. Die DZH wird diese Änderungen nur aus triftigen Gründen, insbesondere aufgrund neuer technischer Entwicklungen, Änderungen der Rechtsprechung oder sonstiger gleichwertiger Gründen unter Berücksichtigung des vertraglichen Gleichgewichts durchführen. Die geänderten AGB werden dem Kunden schriftlich oder über das Online Kundencenter zur Verfügung gestellt. Sie werden entweder mit Bestätigung des Kunden im Online

Kundencenter oder im Falle schriftlicher oder elektronischer Zusendung wirksam, wenn der DZH nicht innerhalb von zwei Wochen ab Zustellung ein schriftlicher Widerspruch des Kunden eingeht.

12. Schlussbestimmungen

Änderungen, Ergänzungen und die Aufhebung dieser Vereinbarung bedürfen der Schriftform. Gleiches gilt für eine Änderung oder Aufhebung des Schriftformerfordernisses.

Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und den einschlägigen datenschutzrechtlichen Vorgaben genügt.

Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der personenbezogenen Daten/Sozialdaten und der zugehörigen Datenträger ausgeschlossen.

Sämtliche Kommunikation zwischen dem Auftragnehmer und dem Auftraggeber sowie zwischen dem Auftragnehmer und den Aufsichten/Prüfdiensten haben in deutscher Sprache zu erfolgen.

13. Anlage – Technisch-organisatorische Maßnahmen

Eine Dokumentation der technischen und organisatorischen Maßnahmen nach Art. 32 Abs. 1 EU-DSGVO ist Bestandteil dieses Auftrags und liegt dieser Vereinbarung als Anlage anbei. Diese zum Datenschutz getroffenen Maßnahmen unterliegen dem technischen Fortschritt und werden somit fortlaufend aktualisiert.

Anhang 1: Technische und organisatorische Maßnahmen

(Ende der Vereinbarung zur Auftragsverarbeitung)

(Die Vereinbarung ist dem Auftraggeber in Textform übermittelt worden und ohne Unterschrift gültig)