Anlage – Vertrag über eine Auftragsverarbeitung gemäß Art. 28 Datenschutz-Grundverordnung (DS-GVO)

(Abrechnungskunden Gesundheitsfachberufe)

Präambel

Um die Rechte und Pflichten aus dem Auftragsverarbeitungsverhältnis gemäß der gesetzlichen Verpflichtung aus Art. 28 DSGVO zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung.

1. Gegenstand des Auftrags, Art und Zweck der Verarbeitung

1.1. Der Auftragnehmer erbringt Dienstleistungen im Rahmen der Abrechnung von Rezepten für Apotheken und sonstigen Leistungserbringern gegenüber den Kostenträgern gemäß den Vorgaben des Sozialgesetzbuches Fünftes Buch (SGB V) (insb. §§ 300 und 302 SGB V) sowie nach den Vorgaben des Sozialgesetzbuches Elftes Buch (SGB XI) (insb. § 105 SGB XI). Im Übrigen ergibt sich der Gegenstand des Auftrags aus der zwischen den Parteien geschlossenen Dienstleistungsvereinbarung („Hauptvertrag“).

1.2. Der Auftraggeber übermittelt dem Auftragnehmer im Rahmen des Hauptvertrags personenbezogene Daten („Daten“). Diese werden nur im Auftrag und nach dokumentierter Weisung des Auftraggebers gemäß Art. 28 DSGVO (Auftragsverarbeitung) und den nachfolgenden Bestimmungen verarbeitet.

1.3. Die Verarbeitung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen dokumentierten Weisung des Auftraggebers (Art. 28 Abs. 3 lit. a DSGVO) und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44-49 DSGVO erfüllt sind.

2. Dauer des Auftrages

Die Laufzeit dieser Auftragsvereinbarung („Vereinbarung“) entspricht der Laufzeit des jeweiligen Hauptvertrags zwischen Auftraggeber und Auftragnehmer.

3. Art der personenbezogenen Daten und Kategorien betroffener Personen

3.1. Abhängig von der Art der Abrechnung werden die folgenden personenbezogenen Date verarbeitet:

- Alle erforderlichen Daten gemäß der jeweils aktuellen Version der technischen **Anlage 3** und **Anlage 4** zur Vereinbarung zur Datenübermittlung nach § 300 SGB V
- Alle erforderlichen Daten gemäß der jeweils aktuellen Version der **Anlage 1** der technischen Anlage für die maschinelle Abrechnung (elektronische Datenübermittlung) zu den Richtlinien der Spitzenverbände der Krankenkassen nach § 302 Abs. 2 SGB V
- Alle erforderlichen Daten gemäß der jeweils aktuellen Fassung der technischen **Anlage 3** zur Regelung der Datenübermittlung nach § 105 Abs. 2 SGB XI
- Ggf. weitere personenbezogene Daten gemäß den technischen Anlagen zu den §§ 300 und 302 SGB V oder § 105 SGB XI.

3.2. Unabhängig von der Art der Abrechnung werden die folgenden personenbezogenen Daten verarbeitet:

- Versichertenstamm: Name, Geburtsdatum, Anschrift, Versichertennummer
- Arztstamm: Arzt-/Praxisname, Anschrift Arztpraxis, BSNR
- Herstellerstamm: Name, Anschrift
- Gesundheitsdaten

3.3. Kreis der betroffenen Personen:

- Kunden der Auftraggeber bzw. Patienten
- Ärzte, Leistungserbringer
- Beschäftigte bei Leistungserbringern, Lieferanten und Leistungsträgern

4. Verantwortlichkeit und Weisungsbefugnis

4.1. Der Auftraggeber ist für die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich (Art. 4 Nr. 7 DSGVO). Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Etwas Anderes gilt nur in dem in Absatz 2 genannten Umfang. Dem Auftragnehmer ist es gestattet, die ihm übermittelten Daten zu anonymisieren, so dass keine Rückschlüsse auf natürliche Personen mehr möglich sind. Anonymisierte Daten, auf die die datenschutzrechtlichen Vorgaben entsprechend den Ausführungen aus Erwägungsgrund 26 DSGVO keine Anwendung mehr finden, kann der Auftragnehmer für eigene Zwecke verwenden.

4.2. Die Verarbeitung der Daten erfolgt ausschließlich gemäß dem zwischen den Parteien geschlossenen Hauptvertrag und auf dokumentierte Weisung des Auftraggebers, es sei denn es besteht eine anderweitige Verpflichtung durch Unionsrecht oder dem Recht des Mitgliedsstaates, dem der Auftragnehmer unterliegt. Im Falle einer anderweitigen Verpflichtung teilt der Auftragnehmer dem Auftraggeber vor der Verarbeitung unverzüglich die entsprechenden rechtlichen Anforderungen mit.

4.3. Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen.

4.4. Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, informiert er gemäß Art. 28 Abs. 3 S. 3 DSGVO unverzüglich den Auftraggeber. Bis zur Bestätigung oder Änderung der entsprechenden Weisung ist der Auftragnehmer berechtigt, die Durchführung der Weisung auszusetzen.

5. Vertraulichkeit und Verpflichtung zur Geheimhaltung

5.1. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die gemäß Art. 28 Abs. 3 S. 2 lit. b DSGVO auf die Vertraulichkeit sowie gemäß § 35 Abs. 1 SGB I auf das Sozialgeheimnis verpflichtet worden sind 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.

5.2. Im Rahmen der Vereinbarung werden auch Daten verarbeitet, die gemäß § 203 StGB unter ein Berufsgeheimnis fallen. Der Auftragnehmer verpflichtet sich, über Berufsgeheimnisse Stillschweigen zu bewahren und sich nur insoweit Kenntnis von diesen Daten zu verschaffen, wie dies zur Erfüllung der ihm zugewiesenen Aufgaben erforderlich ist. Der Auftraggeber weist den Auftragnehmer darauf hin, dass sich Personen, die an der beruflichen Tätigkeit eines Berufsgeheimnisträgers mitwirken und unbefugt ein fremdes Geheimnis offenbaren, das ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt geworden ist, nach § 203 Abs. 4 S. 1 StGB strafbar machen. Zudem macht sich eine mitwirkende Person nach § 203 Abs. 4 S. 2

StGB strafbar, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde.

5.3. Der Auftragnehmer stellt sicher, dass alle mit der Verarbeitung von dem Berufsgeheimnis unterliegenden Daten des Auftraggebers befassten Beschäftigten und andere für den Auftragnehmer tätigen Personen (z.B. Subunternehmer), die damit befasst sind, sich in Textform dazu verpflichtet haben, die ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenen Berufsgeheimnisse nicht unbefugt zu offenbaren und sie über die mögliche Strafbarkeit nach § 203 Abs. 4 StGB belehrt wurden. Der Auftraggeber weist den Auftragnehmer darauf hin, dass sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar macht, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, und die mitwirkende Person nicht dafür Sorge getragen hat, dass die weitere mitwirkende Person zur Geheimhaltung verpflichtet wurde.

5.4. Der Auftragnehmer ist nach Ziffer 7 dieser Vereinbarung berechtigt, Unterauftragnehmer zur Vertragserfüllung heranzuziehen. Im Ausland dürfen Unterauftragnehmer zur Vertragserfüllung nur dann herangezogen werden, wenn der dort bestehende Schutz der Geheimnisse dem Schutz im Inland vergleichbar ist. Der Auftragnehmer wird etwaige Unterauftragnehmer sorgfältig auswählen und diese, soweit sie im Rahmen ihrer Tätigkeit Kenntnis von fremden Geheimnissen im Sinne dieser Vereinbarung erlangen könnten, zum Stillschweigen verpflichten. Der Auftragnehmer wird ferner etwaige Unterauftragnehmer dazu verpflichten, sämtliche von diesen eingesetzten Personen und etwaige weitere Unterauftragnehmer, die bestimmungsgemäß mit Geheimnisschutzdaten in Berührung kommen oder bei denen dies nicht auszuschließen ist, nach den zuvor genannten Grundsätzen zur Verschwiegenheit zu verpflichten und über die Folgen einer Pflichtverletzung zu belehren. Diese Verpflichtung gilt für sämtliche weitere Unterbeauftragungen.

6. Datensicherheit

6.1. Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen zum angemessenen Schutz der personenbezogenen Daten gemäß Art. 28 Abs. 3 lit. c DSGVO in Verbindung mit Art. 32 Abs. 1 DSGVO, um die Sicherheit der Verarbeitung im Auftrag zu gewährleisten. Dazu wird der Auftragnehmer

- die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen,
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen, sicherstellen sowie
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung unterhalten.

6.2. 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.

6.3. Die Vertragsparteien vereinbaren die in dem **Anlage 1** „Technische und organisatorische Maßnahmen“ zu dieser Vereinbarung niedergelegten konkreten Datensicherheitsmaßnahmen.

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.

7. Einbeziehung weiterer Auftragsverarbeiter (Subunternehmer)

7.1. Als Subunternehmer im Sinne dieser Regelung gelten vom Auftragnehmer beauftragte Auftragsverarbeiter, deren Dienstleistungen sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht dazu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen und Reinigung in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

7.2. Die Auslagerung auf Subunternehmer oder der Wechsel des bestehenden Subunternehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Subunternehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten schriftlich oder in Textform gegenüber dem Auftragnehmer Einspruch gegen die geplante Auslagerung erhebt.

und, soweit zutreffend, die Vorgaben der Ziffer 5 dieser Vereinbarung eingehalten werden.

7.3. Mit dem Subunternehmer ist eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 3 und 4 DSGVO abzuschließen, die den Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit dieser Vereinbarung entspricht. Der Auftraggeber ist berechtigt, beim Auftragnehmer Einsicht in dessen Verträge mit Subunternehmern zu nehmen.

7.4. Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Subunternehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. Die durch den Auftraggeber zum Zeitpunkt des Vertragsschlusses genehmigten Subunternehmer sind in der **Anlage 2** zu diesem Vertrag aufgelistet.

8. Unterstützung bei der Wahrung der Betroffenenrechte

8.1. Der Auftragnehmer ist verpflichtet, den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Wahrung der in Art. 12 bis 22 DSGVO genannten Rechte der betroffenen Personen zu unterstützen (Art. 28 Abs. 3 S. 2 lit. e DSGVO).

8.2. Der Auftragnehmer darf personenbezogene Daten nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Auskünfte an Dritte oder betroffene Personen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

8.3. Soweit eine betroffene Person sich unmittelbar an den Auftragnehmer wendet, um ihre Rechte gemäß Art. 12 bis 22 DSGVO geltend zu machen, wird der Auftragnehmer das Ersuchen unverzüglich an den Auftraggeber weiterleiten.

9. Unterstützung bei Dokumentations- und Meldepflichten

9.1. Wenn dem Auftragnehmer eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Auftraggeber unverzüglich Art. 28 Abs. 3 lit. f, Art. 33 Abs. 2 DSGVO). Das Gleiche gilt, wenn beim Auftragnehmer beschäftigte Personen gegen diese Vereinbarung verstoßen.

9.2. Nach Absprache mit dem Auftraggeber trifft der Auftragnehmer unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen.

9.3. Der Auftragnehmer unterstützt den Auftraggeber mit allen ihm zur Verfügung stehenden Informationen bei der Erfüllung der Meldepflichten gegenüber der zuständigen Aufsichtsbehörde gemäß Art. 33 DSGVO und ggf. gegenüber den von der Verletzung des Schutzes personenbezogener Daten Betroffenen gemäß Art. 34 DSGVO.

9.4. Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Auftragnehmer den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten.

10. Beendigung des Auftrags

10.1. Nach Abschluss der Erbringung der Verarbeitungsleistungen hat der Auftragnehmer alle personenbezogenen Daten nach Wahl des Auftraggebers entweder zu löschen oder zurückzugeben, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

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

11. Kontrollrecht des Auftraggebers

11.1. Der Auftraggeber ist berechtigt, vor Beginn der Verarbeitungsleistungen und währenddessen regelmäßig die technischen und organisatorischen Maßnahmen sowie die Einhaltung dieser Vereinbarung und datenschutzrechtlicher Vorgaben zu kontrollieren. Hierfür kann er z. B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers sowie die Einhaltung dieser Vereinbarung nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.

11.2. Der Auftragnehmer ist verpflichtet, dem Auftraggeber zu den üblichen Geschäftszeiten Zutritt zu den Räumlichkeiten zu gewähren, in denen die Daten des Auftraggebers physisch oder elektronisch verarbeitet werden. Der Auftraggeber stimmt die Durchführung der Inspektionen mit dem Auftragnehmer so ab, dass der Betriebsablauf beim Auftragnehmer so wenig wie möglich beeinträchtigt wird. Vor Ort Kontrollen sind grundsätzlich vier Wochen vor der Durchführung der Kontrolle anzukündigen. Der Auftraggeber wird vor Ort Kontrollen nicht häufiger als einmal jährlich durchführen, soweit eine Kontrolle aufgrund besonderer Umstände nicht zwingend erforderlich ist. Die Umstände sind dem Auftragnehmer darzulegen.

11.3. Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der technischen und organisatorischen Maßnahmen sowie der Einhaltung dieser Vereinbarung und datenschutzrechtlicher Vorgaben zur Verfügung. Zu diesen Informationen gehören insbesondere aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, externe Sachverständige, IT-Sicherheits- oder Datenschutzauditoren) und geeignete Zertifizierung (z.B. nach BSI-Grundschutz). Der Auftragnehmer erteilt dem Auftraggeber unverzüglich konkrete Auskunft im Einzelfall.

12. Haftung

Auftraggeber und Auftragnehmer haften im Außenverhältnis nach Art. 82 Abs. 1 und 4 DSGVO für den materiellen und immateriellen Schaden, den eine Person wegen eines Verstoßes gegen die DSGVO erleidet. Sind für einen solchen Schaden sowohl der Auftraggeber als auch der Auftragnehmer verantwortlich, haften die Parteien im Innenverhältnis für diesen Schaden entsprechend ihres Anteils an der Verantwortung. Nimmt eine Person in einem solchen Fall eine Partei ganz oder überwiegend auf Schadensersatz in Anspruch, so kann diese von der jeweils anderen Partei Freistellung oder Schadloshaltung verlangen, soweit es ihrem Anteil an der Verantwortung für den Schaden entspricht.

13. Datenschutz bei kirchlichen Einrichtungen

13.1. Soweit es sich beim Auftraggeber um eine kirchliche Einrichtung im Sinne des § 3 des Gesetzes über den Kirchlichen Datenschutz (KDG) oder um eine Einrichtung im Sinne des § 3 der Kirchlichen Datenschutzregelung der Ordensgemeinschaft päpstlichen Rechts (KDR-OG) handelt, ist dem Auftragnehmer bekannt, dass der Auftraggeber den datenschutzrechtlichen Bestimmungen des KDG bzw. der KDR-OG unterliegt. Der Auftragnehmer bestätigt die Kenntnis dieser Regelungen und deren Beachtung.

13.2. Soweit es sich beim Auftraggeber um eine kirchliche Stelle im Sinne des § 2 des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) handelt, ist dem Auftragnehmer bekannt, dass der Auftraggeber den datenschutzrechtlichen Bestimmungen des DSG-EKD unterliegt. Der Auftragnehmer unterwirft sich gemäß § 30 Absatz 5 Satz 3 DSG-EKD der kirchlichen Datenschutzaufsicht. Die Unterwerfung erstreckt sich auf die Aufgaben und Befugnisse der kirchlichen Datenschutzaufsicht nach §§ 43, 44 EKD-Datenschutzgesetz.

14. Schlussbestimmungen

14.1. Überlassene Datenträger und Datensätze verbleiben im Eigentum des Auftraggebers.

14.2. Sollten einzelne oder mehrere Regelungen dieser Vereinbarung unwirksam sein, so wird die Wirksamkeit der übrigen Vereinbarung hiervon nicht berührt. Für den Fall der Unwirksamkeit einzelner oder mehrere Regelungen werden die Vertragsparteien die unwirksame Regelung unverzüglich durch eine solche Regelung ersetzen, die der unwirksamen Regelung wirtschaftlich und datenschutzrechtlich am ehesten entspricht.

14.3. Im Falle eines Widerspruchs zwischen dem Hauptvertrag und dieser Vereinbarung geht diese Vereinbarung vor, soweit der Widerspruch die Verarbeitung personenbezogener Daten betrifft.

14.4. Die folgenden Anhänge sind Bestandteil dieser Vereinbarung:

- **Anlage 1** (technische und organisatorische Maßnahmen)
- **Anlage 2** (Unterauftragnehmer)

Technische und organisatorische Maßnahmen gem. Art. 32 Abs. 1 DSGVO (Anlage 1 zum Vertrag über eine Auftragsverarbeitung)

1. Maßnahmen zu Gewährleistung der Vertraulichkeit

1.1 **Zutrittskontrolle** Soll verhindern, dass Unbefugte räumlich Zugang zu Datenverarbeitungsanlagen erhalten. Maßnahmen zur Gebäude- und Raumsicherung.	Zutreffend (falls ja, bitte ankreuzen)
Schließsystem/ Schließanlage	☒
Sorgfältige Auswahl externer Wachdienst	☒
Alarmanlage	☒
Verbindung Alarmanlage zu Wachdienst/ Polizei	☒
Lichtschranken/ Bewegungsmelder	☒
Verbindung Bewegungsmelder zu Wachdienst/ Polizei	☒
Videoüberwachung im NOVENTI Rechenzentrum Tomannweg 6, München	☒
Biometrische Zutrittskontrolle	☐
Wachdienst vor Ort/ Sicherung außerhalb der Arbeitszeiten	☒
Personenüberprüfung bei Pförtner /Empfang	☐
Berechtigungsausweise	☒
Besucherausweise	☒
Protokollierung von Besucherzutritten / Besucherbuch	☒
Begleitung von Besucherzutritten durch eigene Mitarbeiter	☒
Elektronische Zutrittscodekarten/ Zutrittstransponder	☒
Schlüsselregelung	☒
Zutrittsberechtigungskonzept	☒
Abgestufte Sicherheitsbereiche und kontrollierter Zutritt	☒
Gesicherter Eingang für An- und Ablieferungen	☒
Gesondert gesicherter Zutritt zum Serverraum	☒
Gesondert gesicherter Zutritt zum Rechenzentrum	☒
Arbeitsanweisungen /Richtlinien bzgl. des Verschließens von Räumlichkeiten bei Verlassen/Arbeitsende	☒
Sorgfältige Auswahl von Reinigungspersonal	☒
Sonstiges: Klicken Sie hier, um Text einzugeben.	☐

1.2 **Zugangskontrolle** Soll den Zugang Unbefugter zu Datenverarbeitungssystemen und deren unbefugte Nutzung verhindern. Systemabsicherung	Zutreffend (falls ja, bitte ankreuzen)
Zuordnung von Benutzerrechten	☒
Erstellen von Benutzerprofilen	☒
Berechtigungsmanagement	☒
Dokumentierter Prozess zur Rechtevergabe bei Neueintritt von Mitarbeitern	☒
Dokumentierter Prozess zum Rechteentzug bei Abteilungswechseln von Mitarbeitern	☒
Dokumentierter Prozess zum Rechteentzug bei Austritt von Mitarbeitern	☒
Funktionelle und/oder zeitlich limitierte Vergabe von Benutzerberechtigungen	☒
Verwendung von individuellen Passwörtern	☒
Login mit Benutzername und Passwort	☒
Login mit biometrischen Daten	☐
Separates BIOS-Passwort	☒
Automatische passwortgesicherte Sperrung des Bildschirms nach Inaktivität (Bildschirmschoner)	☒
Passwortrichtlinie mit Mindestvorgaben zur Passwortkomplexität:	☒
Mindestens 8 Ziffern	☒
Groß- und Kleinschreibung, Sonderzeichen, Zahl (davon mind. 4 Kriterien)	☒
Verhinderung von Trivialpasswörtern (z.B. Passwort1, Passwort2, 123456, qwertz)	☒
Passworthistorie	☐
Verhinderung von PW nach positivem Abgleich mit Wörterbüchern	☐
Eingabebeschränkung bestimmter Sonderzeichen zur Verhinderung von SQL-Injections	☒
Automatische Sperrung von Nutzeraccounts nach mehrfacher Fehleingabe von Passwörtern	☒
Angemessen sicheres Verfahren zum Zurücksetzen von Passwörtern	☒
Sonstiges: (z.B. Nutzung von Fido2)	☐
Hashing von gespeicherten Passwörtern	☒
Hashes werden „gesalzen“ (Salt) oder „gepfeffert“(Pepper)	☐
Verschlüsselung von Netzwerken	☒
Verschluss von Datenverarbeitungsanlagen (z.B. verschlossener Cage für Server)	☒
Sperrung von externen Schnittstellen (z.B. USB)	☐
Programmprüfungs- und Freigabeverfahren bei Neuinstallationen	☒
Verwendung von Intrusion-Prevention-Systemen	☐
Nutzung von VPN-Technologie	☒
Einsatz von Anti-Viren-Software: Server	☒

Einsatz von Anti-Viren-Software: Clients	☒
Einsatz einer Software-Firewall	☐
Einsatz einer Hardware-Firewall	☒
Mobile-Device-Management	☒
Aufbewahrung personenbezogener Daten/Datenträgern in verschließbaren Sicherheitsschränken oder in gesondert gesicherten Räumen	☒
Regelung zum Home Office / zu Telearbeit	☒
Sonstige Maßnahmen: Klicken Sie hier, um Text einzugeben.	☐

1.3 **Zugriffskontrolle** Soll unerlaubte Tätigkeiten in Datenverarbeitungssystemen außerhalb eingeräumter Berechtigungen verhindern.	Zutreffend (falls ja, bitte ankreuzen)
Nutzung eines Berechtigungskonzepts	☒
Minimaler Einsatz von Administratoren-Konten	☒
Trennung von Berechtigungsbewilligung (organisatorisch) und Berechtigungsvergabe (technisch)	☒
Regelung zur Wiederherstellung von Daten aus Backups (wer, wann, auf wessen Anforderung)	☒
Aufbewahrung von Datensicherungen (z.B. Bänder, CDs) im zutrittsgeschützten Safe	☒
Regelmäßige Überprüfung von Berechtigungen	☒
Beschränkung der freien und unkontrollierten Abfragemöglichkeit von Datenbanken	☒
Regelmäßige Auswertung von Protokollen (Logfiles)	☒
Zeitliche Begrenzung von Zugriffsmöglichkeiten	☒
Teilzugriffsmöglichkeiten auf Datenbestände und Funktionen (Read, Write, Execute)	☒
Protokollierung von Dateizugriffen	☐
Protokollierung von Dateilöschungen	☐
Protokollierung von Dateiveränderungen	☐
SPAM-Filter	☒
Intrusiondetection (IDS)	☐
Software für das Security Information and Event Management (SIEM)	☐
Beschränkter Zugriff auf LogFiles (nur Log-Admin)	☒
Speicherung von Log-Files auf dediziertem LogFile-Server	☒
Verschlüsselte Speicherung der Daten	☒
verwendete Verschlüsselungsalgorithmen:	☒
AES (128/256 bit)	☒
RSA (1024/2048 bit)	☐
Sonstiges:	☐
Verwendete Hash-Funktion:	☒
SHA2 (256, 384, 512 bit)	☒
SHA3	☒
bcrypt	☐
Andere Verfahren:	☐
Hashes werden „gesalzen“ (Salt) oder „gepfeffert“(Pepper)	☐
Kontrollierte Vernichtung von Daten:	
Shredder (Cross-Cut, mindestens Stufe 3, DIN 66399)	☐
Verschlossene Behältnisse aus Metall (sog. Datenschutztonnen), Entsorgung durch Dienstleister	☒
Datenträgerentsorgung - Sichere Löschung von Datenträgern (DIN 66399):	☐
Peter-Gutmann-Algorithmus – 35-faches Überschreiben	☐
Physikalische Zerstörung (z.B. Shredder bei Partikelgrößen bis max. 1000 Quadrat-Millimeter)	☐
Entmagnetisierung durch thermische Zerstörung (Erhitzung der Magnetplattenoberfläche über die Curie-Temperatur der verwendeten Beschichtung hinaus)	☐
Entmagnetisierung mittels eines Degaussers	☐
Sonstiges Vernichtungsverfahren:	☐
Richtlinie zur Datenvernichtung	☒
Clean Desk-Policy	☒
Sonstige Maßnahmen: Klicken Sie hier, um Text einzugeben.	☐

1.4 **Auftragskontrolle** Soll sicherstellen, dass Daten, die im Auftrag durch Dienstleister (Subauftragnehmer) verarbeitet werden, nur gemäß der Weisung des Auftraggebers verarbeitet werden.	Zutreffend (falls ja, bitte ankreuzen)
Vertragsgestaltung gem. gesetzlichen Vorgaben (Art. 28 DSGVO)	☒
Zentrale Erfassung vorhandener Dienstleister (einheitliches Vertragsmanagement)	☒
Vorabkontrollen beim Auftragnehmer vor Vertragsbeginn	☒
Regelmäßige Kontrollen beim Auftragnehmer nach Vertragsbeginn (Während Vertragsdauer)	☒
Vor-Ort-Kontrollen beim Auftragnehmer	☒
Überprüfung des Datensicherheitskonzepts beim Auftragnehmer	☒
Sichtung vorhandener IT-Sicherheitszertifikate der Auftragnehmer	☒
Auftragnehmer hat Datenschutzbeauftragten benannt	☒
Erteilung von Weisungen zur Verbesserung des Datenschutzes ggü. Auftragnehmer	☒
Sonstige Maßnahmen: Klicken Sie hier, um Text einzugeben.	☐

1.5 **Trennungskontrolle** Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt voneinander zu verarbeiten.	Zutreffend

	(falls ja, bitte ankreuzen)
Trennung von Kunden (Mandantenfähigkeit des verwendeten Systems)	☒
Physikalische Datentrennung (z.B. unterschiedliche Systeme oder Datenträger)	☐
Logische Datentrennung (z.B. auf Basis von Kunden- oder Mandantennummern)	☒
Datensicherungen der Auftraggeber-Daten auf separaten Datenträgern (ohne Daten anderer Kunden)	☒
Berechtigungskonzept, das der getrennten Verarbeitung der Auftraggeber-Daten von Daten anderer Kunden Rechnung trägt	☒
Trennung von Entwicklungs-, Test- und Produktivsystem	☒
Zuordnung von Datensätzen zu Zweckattributen	☐
Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei & Speicherung auf einem anderen System	☐
Sonstige Maßnahmen: Klicken Sie hier, um Text einzugeben.	☐

2. Maßnahmen zur Gewährleistung der Integrität

2.1 **Weitergabekontrolle** Soll die Sicherheit der Daten bei elektronischer Übertragung und Datentransport und die Nachvollziehbarkeit der Weitergabe gewährleisten.	Zutreffend (falls ja, bitte ankreuzen)
Wie werden Daten zwischen Verantwortlichem und Dritten übermittelt?	
VPN-Verbindung	☒
Secure File Transfer Protocol (sftp)	☒
Citrix-Verbindung	☒
E-Mail-Verschlüsselung	☒
SMIME	☐
OpenPGP	☒
E-Mail Versand mit verschlüsselten ZIP-Dateien	☒
Datenaustausch über https-Verbindung	☒
verwendetes Verschlüsselungsprotokoll:	
TLS 1.3	☒
Sonstige Versendungsart: Gem. SGB V	☒
verwendete Verschlüsselungsalgorithmen:	
AES (128/256 bit)	☒
RSA (1024/2048 bit)	☐
Diffie-Hellmann	☐
Sonstiges:	☐
Nutzung von Signaturverfahren	☐
Verwendetes Signaturverfahren:	
RSA	☐
ElGamal	☐
DSA	☐
Sonstige: PGP, eigene	☒
Digitales Signieren von Makros	☐
Dokumentierte Verwaltung von Datenträgern, Bestandskontrolle	☐
Verschlüsselung vertraulicher Datensätze	☒
Verschlüsselung mobiler Datenträger (z.B. Laptop-Festplatten, externe Festplatten, USB-Sticks)	☒
Verbot der Mitnahme von Taschen und sonstigen Gepäckstücken sowie Mobiltelefonen in Sicherheitsbereiche	☐
Regelung zur Anfertigung von Datensatz-Kopien	☐
Erstellen von Sicherungskopien von Datenträgern, die transportiert werden müssen	☐
Dokumentation der Stellen, an die eine Übermittlung vorgesehen ist, sowie der Übermittlungswege	☒
Direktabholung, Kurierdienst, Transportbegleitung	☒
Vollständigkeits- und Richtigkeitsprüfung	☒
Sonstige Maßnahmen: Klicken Sie hier, um Text einzugeben.	☐

2.2 Eingabekontrolle Soll gewährleisten, dass Nachvollzogen werden kann, ob, wer, wann personenbezogene Daten in Datenverarbeitungssysteme eingeben, geändert oder gelöscht hat.	Zutreffend (falls ja, bitte ankreuzen)
Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	☒
Manuelle oder automatisierte Auswertung der Protokolle	☒
Differenzierte Benutzerberechtigungen:	☒
Einzelne Benutzernamen, keine Benutzergruppen	☒
Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts	☒
Feldzugriff bei Datenbanken	☒
Organisatorische Festlegung von Eingabezuständigkeiten	☒
Verpflichtung auf das Datengeheimnis	☒
Über OS-Standard hinausgehendes Log-Konzept	☒
Dezidierter Logserver	☒
Regelung der Zugriffsberechtigungen für Logserver (LogAdmin)	☒
Regelung zu Aufbewahrungsfristen für Revision/Nachweiszwecke	☒
Sonstige Maßnahmen: Klicken Sie hier, um Text einzugeben.	☐

3. Maßnahmen zur Gewährleistung der Verfügbarkeit & Belastbarkeit

3.1 **Verfügbarkeitskontrolle** Soll Daten gegen zufällige Zerstörung oder Verlust schützen.	Zutreffend (falls ja, bitte ankreuzen)
Brandmeldeanlagen in Serverräumen	☒
Rauchmelder in Serverräumen	☒
Brandschutztüren an papierverarbeitenden Standorten und im Rechenzentrum	☒
Wasserlose Brandbekämpfungssysteme in Serverräumen	☒
Wassersensoren in Serverräumen - Wasserableitung	☒
Blitz-/ Überspannungsschutz	☒
Klimatisierte Serverräume	☒
Serverräumlichkeiten in separaten Brandabschnitt	☒
Unterbringung von Backupsystemen in separaten Räumlichkeiten und in separatem Brandabschnitt	☒
Serverräume nicht unter oder neben sanitären Anlagen	☒
Zutrittsbegrenzung bei Serverräumen auf notwendiges Personal	☒
Alarmmeldung bei unberechtigtem Zutritt zu Serverräumen	☒
Lagerung von Archiv-Speichermedien unter notwendigen Lagerbedingungen (Klimatisierung, Schutzbedarf etc.)	☒
CO2-Feuerlöscher in unmittelbarer Nähe der Serverräume	☒
USV-Anlage (Unterbrechungsfreie Stromversorgung)	☒
Stromgenerator	☒
Feuerfeste Schränke	☐
Datenschutztresor	☒
Dokumentiertes Datensicherungs- und Backupkonzept	☒
Durchführung von Datensicherungen und Erstellen von Backups	☒
Regelmäßige Tests zur Datenwiederherstellung	☒
Spiegeln der Festplatten (z.B. RAID)	☒
Getrennte Partitionen für Betriebssystem und Daten	☐
Havariearchiv (Auslagerung von Daten)	☐
Notfallplan vorhanden (BSI-Standard 100-4)	☒
Gewährleistung der langfristigen technischen Lesbarkeit von Backupspeichermedien	☒
Sonstige Maßnahmen: Klicken Sie hier, um Text einzugeben.	☐

3.2 Belastbarkeit (Widerstandsfähigkeit und Ausfallkontrolle) Soll Systeme befähigen, mit risikobedingten Veränderungen umgehen zu können und Toleranz und Ausgleichsfähigkeit gegenüber Störungen aufzuweisen.	Zutreffend (falls ja, bitte ankreuzen)
Redundante Stromversorgung	☒
Redundante Datenanbindung	☒
Redundante Klimatisierung	☒
Ausweich-Rechenzentren vorhanden (Hot- bzw. Cold-Stand-by?): Hot	☒
sonstige redundante Systeme/Verfahren:	☐
Einsatz einer hochverfügbaren SAN-Lösung (Storage Area Network)	☒
Computer Emergency Response Team (CERT)	☐
Einsatz von Lastenverteilung (Load Balancing)	☒
Abgrenzung kritischer Komponenten	☒
Durchführung von Penetrationstests	☒
Systemhärtung (Deaktivierung nicht erforderlicher Komponenten)	☒
Unverzügliche und regelmäßige Aktivierung von verfügbaren Soft- und Firmwareupdates	☒
Regelmäßige Sensibilisierung der Mitarbeiter (mind. jährlich)	☒
Prozess zur unverzüglichen Meldung von Vorkommnissen an die IT ist allen Mitarbeitern bekannt	☒
Abschluss einer Cyber-Versicherung	☒
Sonstige Maßnahmen: Klicken Sie hier, um Text einzugeben.	☐

4. Cloudlösungen bei Partnerunternehmen

Unsere Partner sind sorgfältig ausgewählt und verfügen über entsprechende Zertifizierungen.

5. Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung

5.1 Kontrollverfahren Soll die Wirksamkeit der Datensicherheitsmaßnahmen gewährleisten.	Zutreffend (falls ja, bitte ankreuzen)
Verarbeitungsverzeichnisse (Art. 30 I und II DSGVO) werden jährlich aktualisiert	☒
Meldung neuer/veränderter Datenverarbeitungsverfahren an den Datenschutzbeauftragten	☒
Meldung neuer/veränderter Datenverarbeitungsverfahren an den IT-Sicherheitsbeauftragten	☒
Prozesse zur Meldung neuer/veränderter Verfahren sind dokumentiert	☒
Prüfung der Wirksamkeit getroffener Sicherheitsmaßnahmen mind. jährlich	☒
Bei negativen Feststellungen im Rahmen der zuvor gen. Überprüfung werden die Sicherheitsmaßnahmen risikobezogen angepasst	☒
Prozess zur Reaktion auf Sicherheitsverletzungen (Angriffe) und Systemstörungen existiert (Incident-Response-Management)	☒
Dokumentation von Sicherheitsvorfällen	☒
Einsatz Security Intelligence	☒

Sicherheitszertifizierungen (ISO 27001, BSI IT-Grundschutz etc.)	☒
Sonstige Maßnahmen: Klicken Sie hier, um Text einzugeben.	☐

5.2 Sonstiges Datenschutzmanagement	Zutreffend (falls ja, bitte ankreuzen)
Einsatz einer Datenschutzmanagement-Software	☒
Datenschutzbeauftragter benannt	☒
IT-Sicherheitsbeauftragter benannt	☒
Dokumentierter Prozess zum Umgang mit Datenschutzvorfällen	☒
Klare Verantwortlichkeiten bei der Handhabung von Datenschutz- und Sicherheitsvorfällen	☒
Zentrale, für alle Mitarbeiter zugängliche Ablage von Richtlinien/Verfahrensanweisungen	☒
Sonstige Maßnahmen: Klicken Sie hier, um Text einzugeben.	☐

Anlage 2 – Unterauftragnehmer
(Anlage 1 zum Vertrag über eine Auftragsverarbeitung)

Im Zusammenhang mit der Erbringung der vertraglichen Leistungen beauftragt der Auftragnehmer folgende Subunternehmer:

Unterauftragnehmer	**Aufgabenfeld**
Kodak Alaris Germany GmbH Hedelfinger Straße 60, 70327 Stuttgart	Wartung und Reparatur Scanner
Riello UPS GmbH Wilhelm-Bergner-Straße 9b, 21509 Glinde	Wartung Server
Integrated Document Solutions AG (IDS) Niederlassung Villingen Wilhelm-Binder-Str. 19, D-78048 Villingen-Schwenningen Dittmannstraße 44 85540 Gronsdorf	Programmierung Erkennung
Canon Deutschland GmbH Siemensallee 2, 85586 Poing	Service Druckermanagement
NOVENTI HEALTH SE Tomannweg 6 81673 München	IT-Services
Computershare GmbH Hansastr. 15 80686 München	Druck und Versand Mahnungen
Reisswolf GmbH Ziegeleiweg 12 19057 Schwerin	Datenträgervernichtung, Papiervernichtung von sensiblen Daten
Prolistic GmbH Bachweg 8 CH 3054 Schüpfen	Scan- und Sortiersysteme
Trenkwalder Business Solution GmbH Werner-Eckert-Straße 6 81829 München	Unterstützung des Kundenservices
S&H Communication GmbH Haagstraße 1 76698 Ubstadt-Weiher	Callcenterleistungen bei Routing und Erfassung der Kundenanfrage mittels Ticketsystem
expertcloud.de GmbH Mehringdamm 55 1096L Berlin	Erbringung von Dienstleistung im Bereich Inbound Call- und Ticketbearbeitung

Informationen über die Erhebung und Verarbeitung Ihrer personenbezogenen Daten

Mit den nachstehenden Informationen erhalten Sie einen Überblick über die Erhebung und Verarbeitung Ihrer personenbezogenen Daten im Rahmen der Rezeptabrechnung und damit verbundener Dienste durch die NOVENTI HealthCare GmbH (NHC).

1. Wer ist für die Datenverarbeitung verantwortlich?

Verantwortlicher für die Datenverarbeitung ist Ihr Vertragspartner:
NOVENTI HealthCare GmbH
Berg-am-Laim-Straße 105
81673 München

2. Wie erreichen Sie den Datenschutzbeauftragten?

Sie erreichen den Datenschutzbeauftragten der NHC unter:
NOVENTI HealthCare GmbH
z. Hd. Datenschutzbeauftragter
Berg-am-Laim-Straße 105
81673 München
Tel.: 089 43184-0
E-Mail: Datenschutz@noventi.de

3. Welche Ihrer personenbezogenen Daten werden durch uns verarbeitet und aus welchen Quellen stammen diese Daten?

3.1 Wir verarbeiten diejenigen personenbezogenen Daten, die Sie uns in Zusammenhang mit der Anbahnung oder der Durchführung eines bestimmten Vertragsverhältnisses übermitteln. Das betrifft insbesondere die Durchführung von Abrechnungs- und damit verbundenen Dienstleistungen. Genaue Informationen können Sie den jeweiligen Vertragsunterlagen entnehmen.

3.2 Des Weiteren erhalten wir von anderen Unternehmen der NOVENTI-Gruppe Ihre personenbezogenen Daten. Dies erfolgt ausschließlich zum Zwecke der Begründung eines neuen Vertragsverhältnisses zwischen den NHC und Ihnen.

4 Für welche Zwecke und auf welcher Rechtsgrundlage verarbeitet die NHC Ihre Daten?

4.1 Auf der Grundlage einer von Ihnen erteilten Einwilligung (Art. 6 Abs. 1 lit. a DSGVO)

Werbung, Marktforschung und Vertrieb: Wenn wir Ihnen Werbung oder Information über unsere Leistungen oder Leistungen anderer Unternehmen der NOVENTI Gruppe zukommen lassen wollen, holen wir, sofern erforderlich, vorab Ihre Einwilligung zur Nutzung Ihre Kontaktdaten ein.

Für die Verarbeitung Ihrer Daten zu Werbe- und Vertriebszwecken ist die NHC und die mit ihr verbundenen Unternehmen der NOVENTI-Gruppe, insbesondere die NOVENTI Health SE, Berg-am-Laim-Straße 105, 81673, München, die NOVENTI Care GmbH, Justus-von-Liebig-Str. 7, 12489 Berlin und die NOVENTI Factory GmbH, Englschalkinger Str. 14, 81925 München, gemeinsam Verantwortliche nach Art. 26 DSGVO. Ihre Betroffenenrechte können Sie jederzeit bei der NHC unter den unter Ziffer 1 angegebenen Kontaktdaten geltend machen.

Zum Zwecke der Marktforschung und der Optimierung des Produktangebots sowie eines bedarfsgerechten Vertriebs der NOVENTI Gruppe werden die folgenden Daten übermittelt und verarbeitet: Adress- und Kontaktdaten der jeweiligen Praxis der sonstige Leistungserbringern, von deren Filialen oder Zweigstellen, des Inhabers und der geschäftlichen Adress- und Kontaktdaten der Mitarbeiter, Informationen zu weiteren Zweigstellen des Inhabers, Geburtsdatum des Inhabers der Praxis, Vertragsdaten zu gebuchten Produkten der NOVENTI HealthCare GmbH einschließlich Vertragslaufzeit und vereinbarte Abrechnungsmarge, Statistiken zur Abrechnung, Bruttorezeptumsatz, Produktausstattung, verwendetes WaWi-System, verwendete Softwarelösungen von der NOVENTI Gruppe, Mitgliedschaften in Verbänden/Kooperationen, Vertragsbeziehungen zu Dritten (z. B. Abholdienst).

Geldwäscheprävention: Mit der Einwilligung unserer Kunden können die im Rahmen der Geldwäscheprävention erforderlichen Daten, die das kontoführende Institut des Kunden im Rahmen der Identifizierung nach dem Geldwäschegesetz (GwG) erhoben hat, von diesem an uns übermittelt werden, damit wir unsererseits den Verpflichtungen nach dem GwG nachkommen können. Das Gleiche gilt für Kopien von amtlichen Dokumenten und Registerauszügen oder -ausdrucken (z. B. Lichtbildausweise, Handelsregisterauszüge, Gewerbenachweise).

4.2 Zur Durchführung vertraglich vereinbarten Leistungen (Art. 6 Abs. 1 lit. b DSGVO)

Vertragserfüllung und -anbahnung: Wir verarbeiten Ihre personenbezogenen Daten, soweit das zur Anbahnung oder Erfüllung von Verträgen erforderlich ist. Ohne die Bereitstellung der erforderlichen Daten ist die Anbahnung und Durchführung von Verträgen nicht möglich.

Selbstständige Vermittlung von Geschäftsbeziehungen: Wir verarbeiten Ihre personenbezogenen Daten auch, wenn wir auf Ihren Wunsch eine Geschäftsbeziehung zu einem anderen Unternehmen der NOVENTI Gruppe vermitteln. Die zu diesen Zwecken erhobenen Daten leiten wir an das oder die Unternehmen der NOVENTI Gruppe weiter, mit dem oder denen eine vertragliche Beziehung eingegangen werden soll. Kommt nach einer durch uns eingeleiteten Vertragsvermittlung eine Vertragsbeziehung direkt mit einem anderen Unternehmen der NOVENTI Gruppe zustande, werden uns die für die interne Abrechnung relevanten Daten zum Zwecke der Verrechnung weitergeleitet.

4.3 Zur Erfüllung rechtlicher Verpflichtungen (Art. 6 Abs. 1 lit. c DSGVO)

Wir verarbeiten Ihre personenbezogenen Daten, wenn wir rechtlich dazu verpflichtet sind.

Geldwäscheprävention: Wir unterliegen den Vorgaben des Geldwäschegesetzes (§ 2 Abs. 1 Nr. 2 GwG). Nach den Bestimmungen des GwG (§§ 10 ff. GwG) sind wir dazu verpflichtet, unsere Kunden, d.h. die Vertragspartner und die wirtschaftlich Berechtigten des Vertragspartners, zu identifizieren. Zu diesem Zweck verarbeiten wir im Einklang mit den gesetzlichen Bestimmungen den Namen, Wohnanschrift, Geburtsdatum und -ort und Staatsangehörigkeit bei natürlichen Personen bzw. Firma, Name oder Bezeichnung, Rechtsform, ggf. Registernummer, Anschrift der Hauptniederlassung sowie die Namen und Daten der Mitglieder des Vertretungsorgans oder der gesetzlichen Vertreter bei juristischen Personen und Personengesellschaften. Zur Erfüllung unserer Aufzeichnungspflicht sind wir außerdem berechtigt, eine Kopie des zur Identifikation vorgelegten Ausweisdokuments (Vorder- und Rückseite) zu speichern (§ 8 Abs. 2 GwG). Zudem prüfen wir im Rahmen der erweiterten allgemeinen Sorgfaltspflichten, ob es sich bei unseren Vertragspartnern oder dem wirtschaftlich Berechtigten um eine politisch exponierte Person, ein Familienmitglied oder eine bekanntermaßen nahestehende Person handelt.

4.4 Zur Wahrung berechtigter Interessen (Art. 6 Abs. 1 lit. f DSGVO)

Direktwerbung: Im Rahmen bestehender Geschäftsbeziehungen verarbeiten wir Ihre personenbezogenen Daten auch, um Ihnen Direktwerbung für eigene ähnliche Produkte und Dienstleistungen mittels elektronischer Post (E-Mail) zukommen zu lassen, soweit Sie der Verarbeitung Ihrer Daten zu diesem Zweck nicht widersprochen haben. Unser berechtigtes Interesse liegt in der Förderung unserer Geschäftstätigkeit.

Vertragserfüllung: Wenn in Zusammenhang mit bestehenden Vertragsverhältnissen auch eine Verarbeitung personenbezogener Daten solcher Personen erforderlich ist, die nicht Vertragspartei sind, erfolgt die Verarbeitung dieser Daten auf der Grundlage unseres berechtigten Interesses. Unser berechtigtes Interesse liegt dann in der Durchführung des jeweiligen Vertragsverhältnisses.

Bonitäts- und geldwäscherechtliche Datenbankprüfung: Zum Zwecke der Beurteilung der Kreditwürdigkeit unserer Kunden, für Abgleiche mit Sanktionslisten („Terrorlistenscreening“) sowie der geldwäscherechtlichen Überprüfung der Kundenangaben werden personenbezogene Daten an Wirtschaftsauskunfteien und Warenkreditversicherer übermittelt und von diesen zur Beurteilung der Kreditwürdigkeit sowie zur unabhängigen Generierung der geldwäscherechtlich erforderlichen Informationen verarbeitet – ggf. im Rahmen eines sog. Score-Verfahrens, bei dem ein von den Wirtschaftsauskunfteien ermittelter Wahrscheinlichkeitswert zur Beurteilung des Kreditrisikos zum Einsatz kommt.

Die folgenden Daten werden in diesem Zusammenhang an Wirtschaftsauskunfteien und/oder Warenkreditversicherer übermittelt:

Unternehmensname, ggf. Anschrift, ggf. Inhabername; Privatauskunft: Anrede, Nachname, Vorname, ggf. Geburtsname, ggf. Geburtsdatum, Straße, Hausnummer, Postleitzahl, Ort.

Wir verarbeiten im Rahmen der Bonitäts- und geldwäscherechtliche Datenbankprüfung zur Beurteilung der Kreditwürdigkeit auch ergänzend personenbezogene Daten zu unseren Kunden (insbesondere Bonitätsbewertung, Daten zu Zahlungsweise und Krediturteil, Strukturdaten, Geschäftszahlen und Beurteilung der Geschäftsverbindung), die uns von der jeweiligen Wirtschaftsauskunftei aus ihrem Datenbestand übermittelt werden.

Unser berechtigtes Interesse liegt in der Durchführung unserer Geschäftstätigkeit bzw. in der Vermeidung von Zahlungsausfällen sowie der Erfüllung geldwäschegesetzlicher Informationsprüfungspflichten.

Anonymisierung: Um bestimmte Datensätze für andere Zwecke – wie z. B. statistische Auswertungen oder die Produktentwicklung - verarbeiten zu können, kann es erforderlich sein, diese Datensätze zuvor zu anonymisieren. Nach einer Anonymisierung können die Daten keiner natürlichen Person mehr zugeordnet werden. Die Anonymisierung erfolgt mit der Hilfe technischer Mechanismen und Hilfsmittel, um die Anonymität der verbleibenden Daten zu gewährleisten.

Refinanzierung: Soweit es im Rahmen einer Refinanzierung erforderlich ist, geben wir Ihre personenbezogenen Daten zum Zwecke der Refinanzierung an Bank- und Kreditinstitute weiter.

5. An wen werden Ihre Daten weitergegeben?

Zur Erfüllung der vertraglichen und gesetzlichen Pflichten der NHC erhalten ggf. auch Dritte Zugriff auf Ihre personenbezogenen Daten. Eine Datenübermittlung an Länder außerhalb der europäischen Union oder des europäischen Wirtschaftsraumes durch NHC findet nur statt, wenn ein Angemessenheitsbeschluss vorliegt oder mit dem Vertragspartner EU-Standardverträge geschlossen sind.

Mögliche Empfänger:

- NOVENTI Health SE (IT-Services, Vertriebsdienstleistungen und weitere Serviceleistungen)
- Warenkreditversicherer und Wirtschaftsauskunfteien (Bonitätsprüfungen),
- Behörden (Geldwäsche), Druckdienstleister (Mahndruck), Abrechnungsschuldner (z. B. Kostenträger), Bank- und Kreditinstitute (Refinanzierung),
- andere Unternehmen der NOVENTI Gruppe, soweit das im Falle der Vermittlung einer Vertragsbeziehung erforderlich ist.

  IT-Dienstleister (insb. Bereitstellung, sowie Wartung und Support datenverarbeitender Systeme)

Sollten Sie weitere Fragen zu den einzelnen Empfängern haben, kontaktieren Sie uns unter:
Datenschutz@noventi.de

6. Wie lange werden Ihre Daten gespeichert?

Die NHC speichert Ihre personenbezogenen Daten, solange es zur Erfüllung der Zwecke, für die die Daten ursprünglich erhoben wurden (insbesondere zur Vertragserfüllung) erforderlich ist. Danach werden Ihre Daten gelöscht, es sei denn, deren weitere Verarbeitung ist zur Einhaltung gesetzlicher Aufbewahrungsfristen, zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder aus anderen gesetzlich vorgesehenen Gründen notwendig. Wenn wir Ihre personenbezogenen Daten auf der Grundlage einer von Ihnen erteilten Einwilligung verarbeiten, speichern wir Ihre Daten spätestens bis zum Widerruf Ihrer Einwilligung, wenn die Zwecke der Verarbeitung nicht vorher entfallen.

7. Welche Rechte haben Sie im Zusammenhang mit der Verarbeitung Ihrer Daten?

Sie haben das Recht auf Auskunft über die von uns über Sie gespeicherten personenbezogenen Daten (Art. 15 DSGVO), das Recht auf Berichtigung Sie betreffender unrichtiger oder unvollständiger personenbezogener Daten (Art. 16 DSGVO), das Recht auf Löschung Ihrer Daten (Art. 17 DSGVO), das Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO), sowie das Recht auf Datenübertragbarkeit (Art. 20 DSGVO).

Sie haben das Recht, Ihre Einwilligung in die Verarbeitung personenbezogener Daten jederzeit mit Wirkung für die Zukunft gegenüber NHC zu widerrufen. Die Rechtmäßigkeit von Verarbeitungen, die vor dem Widerruf erfolgt sind, ist davon nicht betroffen.

Sie haben das Recht, Beschwerde bei der zuständigen Aufsichtsbehörde einzureichen, wenn Sie der Auffassung sind, dass Ihre personenbezogenen Daten entgegen den einschlägigen datenschutz-rechtlichen Bestimmungen verarbeitet werden.

Der Verwendung Ihrer Daten für Werbung unter Verwendung elektronischer Post können Sie jederzeit widersprechen, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen.

Für die Ausübung Ihrer Rechte wenden Sie sich an die NHC unter den unter Ziffer 1 angegebenen Kontaktdaten.