VEREINBARUNG ZUR AUFTRAGSVERARBEITUNG – ANLAGE –

Zwischen Apotheke

– nachfolgend Auftraggeber (Verantwortlicher) –

und CIDA Computerleistungen für Apotheken GmbH

– nachfolgend Auftragnehmer (Auftragsverarbeiter) –

gilt zum bereits bestehenden/noch abzuschließenden Warenwirtschaftsvertrag gemäß dem schriftlich oder in abgestimmter elektronischer Form erteilten Datenverarbeitungsauftrag auf Grundlage der datenschutzgesetzlichen Bestimmungen (s.u. Ziff. VI.1) Folgendes:

I. Gegenstand der Auftragsverarbeitung

1. Der Auftragnehmer erhebt, verarbeitet und nutzt personenbezogene Daten, die auch Sozialdaten nach dem SGB V, XI und XII mit einschließen, für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage dieses Vertrages. Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht.

2. Der Auftrag umfasst Folgendes:

2.1 Gegenstand des Auftrages (Art der Verarbeitung, Art der personenbezogenen Daten):

Erhebung, Speicherung, Veränderung, Übermittlung, Sperrung, Löschung, Nutzung von GKV-Rezeptdaten („personenbezogene Daten, „Gesundheitsdaten“) im Rahmen der Bereitstellung, Betreuung und Wartung einer Apotheken-Warenwirtschaft.

2.2 Dauer des Auftrags

2.2.1 Der Auftrag gilt für die Laufzeit des Warenwirtschaftsvertrages.

2.2.2 Der Auftraggeber kann den Auftrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die Bestimmungen dieser Anlage oder datenschutzgesetzliche Bestimmungen vorliegt, der Auftragnehmer eine den datenschutzgesetzlichen Bestimmungen entsprechende Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

2.3 Kategorien betroffener Personen:

Patienten/Kunden des Auftraggebers, im Status und mit den zugehörigen personenbezogenen Daten als Versicherte der GKV, gesetzlicher Unfallkassen und Berufsgenossenschaften, des SGB XII und des AsylBewLG, Versicherter privater Krankenversicherungen und Selbstzahler.

II. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

1. Für die Beurteilung der Zulässigkeit der Verarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

2. Der Auftraggeber hat das Recht, schriftliche Weisungen im Rahmen dieses Datenverarbeitungsauftrages und/oder des Warenwirtschaftsvertrages gegenüber dem Auftragnehmer zu erteilen.

Weisungsberechtigte Person des Auftraggebers ist, soweit nichts Anderes vereinbart, allein der Apothekeninhaber.

Weisungsempfänger beim Auftragnehmer sind

allein die jeweils vertretungsberechtigten Personen.

3. Der Auftraggeber ist berechtigt, sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen (s. Nr. IV) nach vorheriger Terminvereinbarung zu überzeugen.

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

5. Der Auftraggeber ist verpflichtet, alle im Rahmen der Auftragsverarbeitung erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

III. Pflichten des Auftragnehmers

1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen, nach Weisungen des Auftraggebers sowie den gesetzlichen und liefervertraglichen Bestimmungen, sofern er nicht zu einer anderen Verarbeitung verpflichtet ist (z.B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden). Er hat personenbezogene Daten zu berichtigen, zu löschen und zu sperren, wenn der Auftraggeber dies in der getroffenen Vereinbarung oder einer Weisung verlangt oder vertraglich / gesetzlich vorgesehen ist und sonstige gesetzliche Bestimmungen dem nicht entgegenstehen.

2. Dem Auftragnehmer sind insbesondere Kontrollen nach den gesetzlichen Bestimmungen zu ermöglichen.

3. Soweit ein Verfahrensverzeichnis erstellt wird, hat der Auftragnehmer hieran mitzuwirken. Er hat die erforderlichen Angaben dem Auftraggeber zuzuleiten.

4. Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden – automatisierten – Verwaltung. Eingang und Ausgang werden dokumentiert.

5. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird. Im Zweifel kann der Auftragnehmer die Zulässigkeit der Weisungsaufgabe vom Landesdatenschutzbeauftragten überprüfen lassen.

6. Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber jederzeit - unter Einhaltung einer angemessenen Ankündigungsfrist - dazu berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen, insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen, im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort. Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen mitwirkt. Die in diesem Fall beim Auftragnehmer anfallenden Kosten übernimmt der Auftraggeber. Ohne gesonderte Kostenberechnung ist der Auftragnehmer verpflichtet, den Nachweis für die Umsetzung der technischen und organisatorischen Maßnahmen, die nicht nur den konkreten Auftrag betreffen, durch Vorlage eines ausgefüllten Fragebogens zu erbringen.

7. Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Ablauf der gesetzlichen und der zur Erfüllung des übertragenen Auftrages nötigen Frist zu löschen. Gleiches gilt für Test- und Ausschussmaterial sowie Datensicherungskopien.

   Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegen stehen.

8. Soweit mit der Verarbeitung oder Nutzung personenbezogener Daten des Auftraggebers Unterauftragnehmer einbezogen werden, erfolgt dies grundsätzlich nur unter folgenden Voraussetzungen:

   - Beauftragt der Auftragnehmer Unterauftragnehmer im Sinne der DSGVO, so müssen diese hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahme so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO und zugehöriger Gesetze erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet ist.

- Bei der Einschaltung von Unterauftragnehmern hat der Auftragnehmer den Auftraggeber rechtzeitig vorab zu informieren. Dem Auftraggeber steht in einer solchen Konstellation gesetzlich ein Einspruchsrecht zu. Der Auftraggeber stimmt hiermit zu, dass er das Widerspruchsrecht nur ausüben wird, wenn ein wichtiger datenschutzrechtlicher Grund vorliegt. Sofern eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich sein sollte, steht in einem solchen Fall dem Auftraggeber wie auch dem Auftragnehmer ein Sonderkündigungsrecht zu.

- Zieht ein Auftragnehmer einen weiteren Auftragnehmer hinzu, so hat er diesem dieselben Verpflichtungen aus seinem Vertrag mit dem Auftraggeber aufzuerlegen, die auch für ihn gelten, soweit diese Pflichten für den weiteren Auftragnehmer nicht schon aufgrund anderer Vorschriften verbindlich sind.

- Der Auftraggeber hat das Recht, auf schriftliche Anforderung vom Auftragnehmer Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.

Nicht als Beauftragung von Unterauftragnehmern im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer durch Dritte als Nebenleistung zur Unterstützung bei der Auftragsdurchführung 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. Das Gleiche gilt für vom Auftragnehmer zur Erbringung der vertraglichen Leistungen eingesetzte freie Mitarbeiter als Erfüllungsgehilfen, wenn mit diesen die notwendigen Sorgfalts- und Geheimhaltungspflichten vertraglich vereinbart sind.

9. Vom Auftragnehmer ist ein Beauftragter für den Datenschutz benannt, namentlich Herr Harald Eul, HEC Consulting GmbH, 50321 Brühl, Auf der Höhe 34.

10. Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers das Datengeheimnis zu wahren. Diese besteht auch nach der Beendigung des Vertrages fort.

11. Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO und des BDSG bekannt sind. Er verpflichtet sich, auch folgende für diesen Auftrag relevanten Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen:

Berufsgeheimnis nach § 203 Abs. 1 Nr. 1 StGB

Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu bewahren.

Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und sie auf das Datengeheimnis schriftlich verpflichtet. Der Auftragnehmer überwacht die Einhaltung der hier angegebenen datenschutzrechtlichen Vorschriften. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen. Ausgenommen hiervon sind Auskünfte an Gerichte, Ermittlungs- oder sonstige Behörden, soweit die gesetzliche Pflicht zur Auskunft besteht und erforderliche amtliche Beschlüsse vorliegen.

IV. Technische und organisatorische Maßnahmen (siehe Anhang)

1. Für die auftragsgemäße Bearbeitung der Daten nutzt der Auftragnehmer nach dem Stand der Technik leistungsfähige, daten- und ausfallsichere Einrichtungen der Hard- und Software.

2. Die im Anhang beschriebenen technischen und organisatorischen Maßnahmen werden als verbindlich festgelegt. Hierdurch sollen die gem. Art. 32 DSGVO genannten Sicherheitsziele erreicht werden, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste und deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

Insbesondere gewährleistet der Auftragnehmer

- eine klare Aufgabenverteilung, beispielsweise bei der Vergabe von Zugriffsrechten,

- die Abschottung von Netzen: Es werden Maßnahmen ergriffen werden, um ein unberechtigtes Eindringen in Rechnernetze soweit möglich zu verhindern,

- Maßnahmen zur Verschlüsselung beim elektronischen Datentransfer,

- qualitativ hochwertige Maßnahmen zur Anmeldung am System und sämtlichen datenwesentlichen Anwendungen.

3. Der Auftragnehmer beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung. Er gewährleistet die vertraglich vereinbarten und gesetzlich vorgeschriebenen Datensicherheitsmaßnahmen.

4. Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber auf Anforderung zur Beurteilung mitzuteilen.

5. Soweit die beim Auftragnehmer getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

6. Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit, soweit Daten des Auftraggebers von dem Ereignis betroffen sind. Dies gilt vor allem auch im Hinblick auf eventuelle Informationspflichten des Auftraggebers. Der Auftragnehmer sichert zu, den Auftraggeber bei seinen Pflichten zu unterstützen.

V. Haftung

Es gelten die Regelung des Art. 82 DSGVO.

VI. Sonstiges, Schriftform, Wirksamkeit dieser Anlage

1. Die Vereinbarung erfüllt die Voraussetzungen nach den bisherigen Bestimmungen zur Auftragsdatenverarbeitung gemäß § 11 II BDSG i.d.F. bis 25.05.2018 und ist gemäß der Vorgaben der DSGVO und der hierauf hin zum 25.05.2018 in Kraft tretenden Bestimmungen im BDSG (neu) zur Auftragsverarbeitung angepasst worden. Sollten in Folge der Umsetzung oder Auslegung der Bestimmungen zur Auftragsverarbeitung künftig Änderungen dieser Vereinbarung erforderlich werden, vereinbaren die Parteien hiermit, dass sie diese einvernehmlich umsetzen werden.

2. Für Nebenabreden ist die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

3. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit des Datenverarbeitungsauftrages nebst dieser Anlage und Anhang im Übrigen nicht.

ANHANG:
BESCHREIBUNG DER TECHNISCHEN UND ORGANISATORISCHEN MASSNAHMEN ZU IV. DATENSICHERUNGSMASSNAHMEN

1. Zutrittskontrolle

Unter Zutrittskontrolle werden Maßnahmen verstanden, die Unbefugten den Zutritt zu schutzbedürftigen Räumen verwehren bzw. die Zutritte der Berechtigten protokollieren. Zu den schutzbedürftigen Räumen zählen insbesondere Räume mit Datenverarbeitungsanlagen wie der Serverraum und der Raum für das Operating des Großrechners. Die Gebäudesicherung erfolgt durch Sicherheitsschlösser, Chipkartenleser (s. zu Zutrittsberechtigungen unten), Sicherheitsverglasung, ein Alarmsystem mit Aufschaltung auf eine 24h-Wachzentrale, Videoüberwachung der Außen- und Zugangsbereiche.

Die Zutrittsberechtigungen sind in einem zentralen Zeiterfassungs- und Zutrittskontrollsystem hinterlegt. Dieses System protokolliert neben den Arbeitszeiten der Mitarbeiterinnen und Mitarbeiter auch die individuell vergebenen Zutrittsrechte. Jeder Mitarbeiter verfügt über einen mit seinen jeweiligen Berechtigungen individuell programmierten Transponder.

2. Zugangskontrolle

Unter Zugangskontrolle werden Maßnahmen verstanden, die es nur entsprechend autorisiertem Personal gestatten auf bestimmte IT-Systeme oder IT-Anwendungen zuzugreifen. Momentan wird diese Anforderung durch die Vergabe von nutzerbezogenen Loginnamen und Passwörtern umgesetzt und somit ein unberechtigter Zugriff auf IT-Systeme unterbunden.

3. Zugriffskontrolle

Unter Zugriffskontrolle werden Maßnahmen verstanden, die sicherstellen, dass nur entsprechend berechtigte Mitarbeiterinnen und Mitarbeiter auf bestimmte Daten oder Anwendungen innerhalb eines Datenverarbeitungssystems zugreifen können. Um diese Anforderung umzusetzen wurden für bestimmte IT-Anwendungen ein Rollen- und Rechtemodell eingeführt welches die jeweiligen Zugriffsrechte (Lesen, Schreiben, Ändern, Löschen) der Nutzer definiert, realisiert und die entsprechenden Zugriffe protokolliert. Andere IT-Anwendungen sind mandantenfähig. Somit wird sichergestellt, dass nur bestimmte Nutzergruppen entsprechende Zugriffsrechte bekommen.

4. Weitergabekontrolle

Unter Weitergabekontrolle werden Maßnahmen verstanden, die 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 welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. So werden personenbezogene Daten bei elektronischer Übertragung grundsätzlich nur verschlüsselt oder auf verschlüsselten Transportwegen (https oder SFTP) übermittelt. Dabei wird sichergestellt, dass die Verschlüsselungsalgorithmen dem aktuellen Stand der datenschutzrechtlichen Anforderungen (z.B. bzgl. der Schlüssellänge) entsprechen.

5. Eingabekontrolle

Unter Eingabekontrolle werden Maßnahmen verstanden die sicherstellen, dass nachvollzogen werden kann, welche Mitarbeiter welche Datenbearbeitung zu welchen Zeitpunkten an welchen Datenverarbeitungssystemen und Anwendungen vorgenommen haben. Diese Anforderung wird allein schon durch die Maßnahmen im Kontext der Zugriffskontrolle erfüllt. Durch das personenbezogene Login und die personenbezogene Vergabe von Rollen und Rechten für bestimmte Anwendungen und Tätigkeiten werden die entsprechenden Aktivitäten entsprechend protokolliert. Versuche unbefugten Einloggens oder Überschreitung von Befugnissen werden somit erkannt und nachvollziehbar in entsprechenden Logfiles protokolliert.

6. Verfügbarkeitskontrolle

Unter Verfügbarkeitskontrolle werden alle Maßnahmen verstanden, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Dazu dienen neben den Maßnahmen im Kontext Zutritts-, Zugangs- und Zugriffskontrolle insbesondere die vorgeschriebenen Regelungen zur Datensicherung bis hin zur externen Lagerung der gesicherten Daten. Alle relevanten Rechnersysteme sind durch leistungsfähige unterbrechungsfreie Stromversorgungen gegen einen plötzlichen Stromausfall gesichert. Internetbasierte Angriffe auf die Datenbestände werden durch entsprechende Maßnahmen (z.B. Firewall) verhindert. Die höchstmögliche Verfügbarkeit der Rechnersysteme wird durch Service Level Agreements und Wartungsverträge sichergestellt.

7. Trennungskontrolle

Unter Trennungskontrolle werden Maßnahmen verstanden die sicherstellen, dass insbesondere personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben wurden, nur getrennt verarbeitet werden können um eine übergreifende Profilbildung zu vermeiden.