Vereinbarung zur Auftragsverarbeitung

zwischen

PT-Kunde

- nachstehend Auftraggeber genannt -

und

Pharmatechnik GmbH & Co KG
Münchner Straße 15
82319 Starnberg

- nachstehend Auftragnehmer genannt -

Präambel

Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus dem schuldrechtlichen Vertrag (Hauptvertrag) ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten („Daten“) des Auftraggebers in Berührung kommen können.

1. Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

1.1 Der Gegenstand, Art und Zweck der Auftragsverarbeitung sind im schuldrechtlichen Vertrag (Hauptvertrag) bzw. jeder ihn ablösenden oder ergänzenden weiteren Leistungsvereinbarung zwischen den Vertragsparteien über den gleichen Gegenstand (im Folgenden bezeichnet als „aktuelle Leistungsvereinbarung“) beschrieben. Im Wesentlichen findet die Auftragsverarbeitung im Rahmen der aktuellen Leistungsvereinbarung statt zwecks:

- Systemwartung (einschließlich Fernwartung)
- Datenaustausch in Filialverbünden, sofern vorhanden
- Datenübermittlung an Vertragspartner der Apotheke, nach Maßgabe des Auftraggebers
- Aufbereitung für betriebswirtschaftliche, insbesondere buchhalterische Zwecke

1.2 Die Verarbeitung umfasst die nachfolgend genannten Arten von Daten:

- Personenstammdaten einschl. Abrechnungs- und Zahlungsdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Gesundheitsrelevante Daten als besondere Arten von Daten nach Art. 9 DSGVO.

1.3 Folgende Kategorien von Personen sind von der Verarbeitung betroffen:

- Apotheken-Kunden
- Mitarbeiter von Kunden der Apotheke (z.B. Krankenhaus- oder Heimmitarbeiter)
- Heimbewohner
- Krankenhauspatienten
- Ansprechpartner (wie z.B. Vormund, Angehörige von Apothekenkunden und/oder Heimbewohnern)
- Bei Einsatz vorhandener IT-Infrastruktur ggf. Einsicht in personenbezogene Mitarbeiterdaten der Apotheke.

1.4 Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Vereinbarung nicht darüber hinaus gehende Verpflichtungen ergeben.

2. Anwendungsbereich und Verantwortlichkeit

2.1 Der Auftragnehmer verarbeitet Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im jeweiligen Hauptvertrag sowie aller Ergänzungen vereinbart sind. Der Auftraggeber ist hinsichtlich der Verarbeitung der Daten für die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz, insbesondere für die Rechtmäßigkeit der Datenverarbeitung, verantwortlich.

2.2 Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die über die vertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

3. Pflichten des Auftragnehmers

3.1 Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der dokumentierten Weisungen des Auftraggebers verarbeiten. Sofern der Auftragnehmer durch nationales oder europäisches Recht zu einer hiervon abweichenden Verarbeitung verpflichtet ist, weist er – sofern dies rechtlich zulässig ist – den Auftraggeber vor Beginn der Verarbeitung auf diesen Umstand hin.

3.2 Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird die im **Anhang 1** beschriebenen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen. Die Maßnahmen sollen die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt. Er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

3.3 Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte

Schutzniveau nicht unterschritten wird. Der Auftragnehmer informiert den Auftraggeber durch E-Mail oder über seine Kundeninformationssysteme über eine solche Änderung.

3.4 Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten und der vertraglich geschuldeten Leistung bei der Erfüllung der Anfragen und Ansprüche Betroffener gemäß Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten.

3.5 Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisungen des Auftraggebers zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits- und Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

3.6 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes von Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

3.7 Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

3.8 Der Auftragnehmer gewährleistet, seinen Pflichten nach 32 Abs. 1 lit. d DSGVO nachzukommen und ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

3.9 Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Beschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber, sofern nicht im Vertrag bereits vereinbart.

3.10 Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind. Er verpflichtet sich, auch folgende für diesen Auftrag relevanten Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen: § 203 StGB.

3.11 Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.

4. Pflichten des Auftraggebers

4.1 Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

4.2 Im Falle einer Inanspruchnahme durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich Auftraggeber und Auftragnehmer hinsichtlich der Verifizierung der Aktivlegitimation bei der Abwehr des Anspruches sich gegenseitig zu unterstützen.

4.3 Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

5. Anfragen Betroffener

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer den Betroffenen an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach den Angaben des Betroffenen möglich ist.

6. Nachweismöglichkeiten

6.1 Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in Art. 28 DSGVO und diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach. Zum Nachweis der Einhaltung der vereinbarten Pflichten kann der Auftragnehmer, dem Auftraggeber Zertifikate und Prüfergebnisse Dritter (z.B. nach Art. 42 DSGVO oder ISO 27001) zur Verfügung stellen oder Prüfberichte des betrieblichen Datenschutzbeauftragten.

6.2 Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der Unterzeichnung einer angemessenen Verschwiegenheitserklärung abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

6.3 Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich 6.2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde

einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

6.4 Für die Unterstützung bei der Durchführung einer Inspektion nach 6.2 oder 6.3 darf der Auftragnehmer eine angemessene Vergütung verlangen, sofern nicht Anlass der Inspektion der dringende Verdacht eines Datenschutzvorfalls im Verantwortungsbereich des Auftragnehmers war. In diesem Fall sind die Verdachtsmomente mit der Ankündigung der Inspektion vom Auftraggeber vorzutragen.

7. Subunternehmer (weitere Auftragsverarbeiter)

7.1 Der Auftraggeber stimmt zu, dass der Auftragnehmer Subunternehmer hinzuzieht. Vor der Hinzuziehung oder Ersetzung von Subunternehmern informiert der Auftragnehmer den Auftraggeber mit einer Frist von vier Wochen. Der Auftraggeber kann der Änderung nur aus wichtigem Grund widersprechen. Der Widerspruch hat binnen 14 Tagen schriftlich zu erfolgen und alle wichtigen Gründe ausdrücklich zu benennen. Erfolgt innerhalb der Frist kein Widerspruch, gilt die Zustimmung zur Änderung als gegeben. Liegt ein wichtiger Grund vor, der vom Auftragnehmer nicht durch Anpassung des Auftrages beseitigt werden kann, steht dem Auftragnehmer ein Sonderkündigungsrecht zu. Dieses Sonderkündigungsrecht bezieht sich sowohl auf diese Vereinbarung als auch auf den Hauptvertrag. Über die in **Anhang 2** aufgeführten, bei Vertragsschluss bereits bestehenden, Subunternehmer erfolgt keine gesonderte Information. Ein Widerspruchsrecht des Auftraggebers besteht für diese Subunternehmer nicht.

7.2 Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

7.3 Auf schriftliche Aufforderung des Auftraggebers hat der Auftragnehmer jederzeit Auskunft über die datenschutzrelevanten Verpflichtungen seiner Subunternehmer zu erteilen.

8. Informationspflichten, Schriftformklausel, Rechtswahl

8.1 Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher « im Sinne der DSGVO liegen.

8.2 Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in elektronischer Form erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine

Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

8.3 Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

8.4 Es gilt deutsches Recht.

Anhänge: Anhang 1: Allgemeine technische und organisatorische Maßnahmen nach Art. 32 DSGVO
Anhang 2: Subunternehmer nach Ziff. 7.1

_____, den _____ Starnberg, den 23.04.2025

_____ _____

Auftraggeber (Stempel, Unterschrift) PHARMATECHNIK GmbH & Co. KG
Auftragnehmer

Anhang 1:

Allgemeine technische und organisatorische Maßnahmen nach Art. 32 DSGVO

1. Pseudonymisierung und Verschlüsselung personenbezogener Daten

a. Pseudonymisierung

Die Verarbeitung von Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.

b. Verschlüsselung

Die eingesetzten Verschlüsselungsmethoden ergeben sich aus den folgenden technischen und organisatorischen Maßnahmen.

2. Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen

a. Zutrittskontrolle

Der Auftragnehmer beschränkt den Zugang zu seinen Geschäftsstellen mit DV-Systemen mit Zugriff auf Auftraggeberdaten auf einen definierten Personenkreis.

Die Zutrittskontrolle erfolgt durch:

- Pförtner (an besetzten Eingängen) oder
- Kartenlesegeräte (an unbesetzten Eingängen)

für alle Betriebsgebäude in allen Geschäftsstellen.

Die zentralen IT-Systeme sind in geschützten Räumen so eingerichtet, dass nur Berechtigte Zutritt haben. Der Zutritt für grundsätzlich nicht zum Zutritt berechtigte Mitarbeiter und unternehmensfremde Personen (z.B. Reinigungskräfte, Besucher etc.) erfolgt immer in Begleitung einer berechtigten Person.

Die Angaben zur Zutrittskontrolle beziehen sich auch auf solche Auftraggeberdaten, die im Auftrag des Auftraggebers erhoben, verarbeitet, genutzt, gesperrt oder gelöscht werden sollen.

b. Zugangskontrolle

Der Auftragnehmer verwendet zur Authentifizierung Benutzeraccounts und Passwortschutz gemäß den anerkannten Regeln der Technik. Jeder Berechtigte verfügt über ein eigenes, nur ihm bekanntes Passwort.

Für Passworte sind Prozesse zu ihrer regelmäßigen Änderung eingeführt. Alle Passwörter erfüllen folgende Mindestanforderungen, u.a. mit folgenden Regeln:

- Maximales Kennwortalter 60 Tage

- Minimale Kennwortlänge 6 Zeichen
- Kennwortchronik über 5 Kennworte
- Kontosperrungsschwelle nach 10 versuchen auf 120 Minuten

Der Auftragnehmer speichert Passworte verschlüsselt.

Die Nutzung von IT-Systemen mit Hilfe von Einrichtungen der Datenübertragung durch Unbefugte wird durch folgende Maßnahmen verhindert:

- Mehrstufige Firewall
- VPN mit L2TP/IPSec: AES256-Verschlüsselung mit SHA2 als Hash-Algorithmus.

Alle gemachten Angaben zur Zugangskontrolle beziehen sich auch auf Daten, die vom Auftragnehmer im Auftrag des Auftraggebers erhoben, verarbeitet, genutzt, gesperrt oder gelöscht werden sollen.

c. Zugriffskontrolle

Das Softwaredesign ermöglicht einen Zugriff auf Auftraggeberdaten nur von Accounts aus, die Personen zugeordnet sind.

„Least privilege“: Supportpersonal hat nur Zugriff auf Auftraggeberdaten, wenn dies zur Durchführung ihrer Aufgaben notwendig ist. Der Auftragnehmer beschränkt solche Zugriffe auf jene Personen, die diese Aufgaben im Rahmen ihrer Tätigkeitsbeschreibung durchführen.

Die Vernichtung von Datenträgern, die Auftraggeberdaten enthalten können, erfolgt durch zertifizierte Unterauftraggeber, die eine vollständige und unwiederbringliche Zerstörung garantieren.

d. Weitergabekontrolle

Der Auftragnehmer hat definierte Prozesse für den Zugriff auf Auftraggeberdaten im Einsatz.

Soweit physikalisch Datentransporte stattfinden, werden hierzu portable Speichermedien eingesetzt, die nach folgenden Verfahren verschlüsselt werden:

- ZIP-Komprimierung mit jeweils unterstützter Verschlüsselung, z.B. AES256

Der Auftragnehmer hält angemessene Anti-Malware-Software vor, die sowohl vom Auftraggeber als auch aus öffentlichen Netzen übernommene Daten und Programme überprüft.

Der Auftragnehmer überträgt Auftraggeberdaten grundsätzlich verschlüsselt.

Es werden die folgenden Sicherheitsmaßnahmen verwendet:

- Virenschutz (siehe oben)
- Firewalls (siehe oben)
- VPN (Virtual Private Networks)

e. Eingabekontrolle

Der Auftragnehmer dokumentiert alle relevanten Prozessschritte, die bei Verarbeitung von Auftraggeberdaten anfallen.

f. Trennungskontrolle

Der Auftragnehmer speichert Auftraggeberdaten in mandantenfähigen Datenhaltungen, sodass eine eindeutige Zuordnung von Datensätzen zu verschiedenen Auftraggebern möglich ist.

Produktive Auftraggeberdaten werden getrennt von gleichartigen Daten zum Zweck von Entwicklungen und Tests gespeichert.

3. Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen

Personenbezogene und besondere Arten personenbezogener Daten werden im Rahmen der Auftragsdatenverarbeitung nur als Kopien gehalten, die Originaldaten bleiben immer in den Systemen des Auftraggebers erhalten. Der Auftragnehmer setzt für alle Auftraggeberdaten Backupverfahren nach den anerkannten Regeln der Technik ein, sodass von ihm verarbeitete Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

a. Regelmäßige Überprüfungen der eigenen IT-Systeme

Es findet eine regelmäßige Überprüfung und Qualitätssicherung statt, ob sich der Stand der Technik verändert hat und entsprechender Anpassungsbedarf der IT-Systeme besteht.

Es finden regelmäßig externe Prüfungen der IT-Systeme und/oder der Schutzmaßnahmen statt (z.B. Penetrationstests).

Die eingesetzte Hard- und Software wird regelmäßig auf Funktionsfähigkeit überprüft.

Die Schutzbedarfsklassifizierung für Datenverarbeitungen wird regelmäßig überprüft.

b. Regelmäßige Überprüfungen von Subauftragnehmern (Auftragskontrolle)

Der Auftragnehmer ist berechtigt, Unteraufträge zur Auftragsdatenverarbeitung zu erteilen. Der Auftragnehmer schließt mit Subauftragnehmern, die Auftraggeberdaten bearbeiten, Auftragsverarbeitungsverträge oder Datenschutzvereinbarungen gemäß Art. 28 Abs. 3 S. 1 DSGVO, mit denen der Schutz der Auftraggeberdaten mindestens in dem Maß gewährleistet ist wie durch diese Vereinbarung, ab.

Zu diesem Zweck stellt der Auftragnehmer auch sicher, dass der Auftraggeber das Recht hat, auch bei Unterauftragnehmer die hier vereinbarten Überprüfungen vorzunehmen.

Anhang 2:

Subunternehmer nach Ziffer 7.1

Name	**Anschrift**	**Auftragsinhalt**
TeleService Holding AG	Destouchesstrasse 68 80796 München	Dienstleister für DSL-Lösungen
Deutsches Gesundheitsnetz (DGN)	Niederkasseler Lohweg 181-183 40547 Düsseldorf	Infrastrukturpartner KV-SafeNet
indevis IT-Consulting and Solutions GmbH	Irschenhauser Straße 10 81379 München	Infrastrukturpartner VPN
Microsoft Deutschland GmbH	Konrad-Zuse-Str. 1 85716 Unterschleißheim	Dienstleister German Cloud
Pharmazeutische Datenmanagement + Service GmbH (PDM+S)	Eckdrift 41 19061 Schwerin	Servicepartner Verblisterung
TeamViewer GmbH	Jahnstr. 30 73037 Göppingen	Lieferant Fernwartungssoftware