

Anlage 3

Vereinbarung zur Auftragsverarbeitung

nach Art. 28 DSGVO („AVV“)

Präambel

Für Zwecke dieser AVV wird **gesund.de** im Folgenden als „**Auftragnehmer**“ und der jeweilige **Vertragspartner** als „**Auftraggeber**“ bezeichnet. Dieser AVV konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der *gesund.de CardLink-Vereinbarung zur Implementierung in ein apothekenbetriebenes informationstechnisches System für die Entgegennahme und Einlösung von elektronischen Verordnungen* zwischen dem Auftragnehmer und dem Auftraggeber ergeben (für Zwecke dieses AVV im Folgenden: „**Vereinbarung**“).

Dieser AVV findet nur Anwendung auf die Verarbeitung personenbezogener Daten („**pbD**“) im Zusammenhang mit der Vereinbarung durch den Auftragnehmer im Auftrag des Auftraggebers.

1. Gegenstand, Dauer und Spezifizierung der AVV

- 1.1 Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung sowie Art der Daten und Kategorien Betroffener sind in **Annex 1** beschrieben.
- 1.2 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:
 - Berufsgeheimnis nach § 203 Abs. 1 Nr. 1 StGB.

2. Anwendungsbereich und Verantwortlichkeit

- 2.1 Der Auftragnehmer verarbeitet pbD im Auftrag des Auftraggebers. Der Auftraggeber ist hinsichtlich der Verarbeitung der pbD für die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz verantwortlich, insbesondere für die Rechtmäßigkeit der Datenverarbeitung.
- 2.2 Die Weisungen werden anfänglich durch den vorliegenden AVV 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**“).

Einzelweisungen, die über die vertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Change Request im Sinne der Vereinbarung behandelt.

3. Pflichten des Auftragnehmers

- 3.1 Der Auftragnehmer darf pbD von betroffenen Personen nur im Rahmen dieses AVV 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. Der Auftragnehmer ist berechtigt, Sicherungskopien der pbD des Auftraggebers zu erstellen.
- 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 **Annex 4** beschriebenen technischen und/oder organisatorischen Maßnahmen zum angemessenen Schutz der pbD des Auftraggebers treffen. Die Maßnahmen sollen die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen.
- 3.3 Eine Änderung der getroffenen technischen und/oder organisatorischen Maßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht wesentlich unterschritten wird.
- 3.4 Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner gesetzlichen Verpflichtung und der vertraglich geschuldeten Leistung bei der Erfüllung der Anfragen und Ansprüche Betroffener gemäß Kapitel III der DSGVO sowie bei der Einhaltung der in Artikel 33 bis 36 DSGVO genannten Pflichten.
- 3.5 Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der pbD befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits- und Verschwiegenheitspflicht besteht auch nach Beendigung dieses AVV fort.
- 3.6 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes pbD des Auftraggebers bekannt werden.
- 3.7 Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des AVV anfallende Datenschutzfragen (vgl. **Annex 2**).
- 3.8 Der Auftragnehmer berichtet oder löscht die pbD, 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 Einzelweisung durch den Auftraggeber, sofern nicht in der Vereinbarung bereits vereinbart.

- 3.9 Daten sowie sämtliche sonstige Materialien des Auftraggebers sind nach Ende des AVV auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen, soweit keine gesetzlichen Aufbewahrungspflichten für den Auftragnehmer bestehen.

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 Artikel 82 DSGVO verpflichten sich Auftraggeber und Auftragnehmer, sich hinsichtlich der Verifizierung der Aktivlegitimation und bei der Abwehr des jeweiligen Anspruches gegenseitig zu unterstützen.
- 4.3 Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des AVV anfallende Datenschutzfragen.

5. Anfragen Betroffener Personen

Wendet sich eine betroffene Person mit einem datenschutzrechtlichen Anliegen, z. B. der Geltendmachung eines Betroffenenrechts, an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach den Angaben der betroffenen Person möglich ist.

6. Nachweismöglichkeiten

- 6.1 Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in Artikel 28 DSGVO und dieser AVV niedergelegten Pflichten auf Anforderung des Auftraggebers mit geeigneten Mitteln nach.

Zum Nachweis der Einhaltung der vereinbarten Pflichten kann der Auftragnehmer dem Auftraggeber insbesondere Zertifikate und Prüfergebnisse Dritter (z. B. nach Artikel 42 DSGVO oder nach einer relevanten DIN- und/oder ISO-Norm) oder gegebenenfalls Prüfberichte eines betrieblichen Datenschutzbeauftragten zur Verfügung stellen.

- 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 **Ziffer 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 **Ziffer 6.2** oder **Ziffer 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. Unter-Auftragsverarbeiter (weitere Auftragsverarbeiter)

- 7.1 Der Auftraggeber stimmt zu, dass der Auftragnehmer Unter-Auftragsverarbeiter hinzuzieht.

Diese können auch in einem Drittstaat personenbezogene Daten verarbeiten.

Vor der Hinzuziehung oder Ersetzung von Unter-Auftragsverarbeitern informiert der Auftragnehmer den Auftraggeber mit einer Frist von vier Wochen in Textform (z. B. per Hinweis im Apotheken-Cockpit). Der Auftraggeber kann der Änderung nur aus wichtigem Grund widersprechen. Der Widerspruch hat binnen 14 Kalendertagen nach Zugang der entsprechenden Information zu erfolgen und alle wichtigen Gründe ausdrücklich zu benennen. Erfolgt innerhalb dieser Frist kein Widerspruch, gilt die Zustimmung zur Änderung als erteilt. Liegt ein wichtiger Grund vor, der vom Auftragnehmer nicht durch Anpassung der jeweiligen Datenverarbeitung nach beseitigt werden kann, steht dem Auftragnehmer ein Sonderkündigungsrecht zu. Dieses Sonderkündigungsrecht bezieht sich sowohl auf diesen AVV als auch auf die jeweilige Funktionsvereinbarung nach der Vereinbarung.

Über die in **Annex 3** aufgeführten, bei Abschluss dieses AVV bereits bestehenden, Unter-Auftragsverarbeiter erfolgt keine gesonderte Information. Ein Widerspruchsrecht des Auftraggebers besteht für diese Unter-Auftragsverarbeiter nicht.

- 7.2 Falls pbD an Empfänger in Drittstaaten außerhalb der EU und des EWR übermittelt werden, erfolgt eine solche Datenübermittlung grundsätzlich auf der Grundlage der EU Standardvertragsklauseln.

Der Auftraggeber kann weitere Informationen und die entsprechende Vorlage über die folgende Webseite abrufen:

https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_de

Der Auftragnehmer hat das Recht für die Übermittlung von pbD an Empfänger in Drittstaaten außerhalb der EU und des EWR andere Maßnahmen gemäß Artikeln 44 ff. DSGVO anzuwenden.

Der Auftragnehmer informiert den Auftraggeber entsprechend **Ziffer 7.1**.

- 7.3 Erteilt der Auftragnehmer Aufträge an Unter-Auftragsverarbeiter, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem AVV dem Unter-Auftragsverarbeiter zu übertragen.
- 7.4 Auf schriftliche Aufforderung des Auftraggebers hat der Auftragnehmer jederzeit Auskunft über die datenschutzrelevanten Verpflichtungen seiner Unter-Auftragsverarbeiter zu erteilen.
- 7.5 Nicht als Unterauftragsverhältnisse im Sinne dieses AVV sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben.

Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste und Infrastrukturdienstleister.

Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz pbD zu gewährleisten.

8. Inhaberwechsel

- 8.1 Überträgt der Auftraggeber sein Apothekengeschäft an eine zur Weiterführung der Apotheke befugte Person, die über die Berechtigung sowie die behördliche Erlaubnis iSd. §§ 1, 2 ApoG verfügt ("Inhaberwechsel"), ist es dem Auftraggeber gestattet, die hiesige Vereinbarung an den neuen Inhaber zu übertragen. Der neue Inhaber tritt mit Vollzug des Inhaberwechsels in diese Vereinbarung mit dem Auftragnehmer ein. Der Auftragnehmer erteilt hierzu seine vorweggenommene Zustimmung zur Vertragsübernahme (einschließlich Schuldübernahme) durch den neuen Inhaber.
- 8.2 Der Auftraggeber hat dem Auftragnehmer den Inhaberwechsel mindestens zwei (2) Wochen vor Vollzug unter Vorlage geeigneter Nachweise (insb. behördliche Erlaubnis, Übergabevertrag) anzuzeigen.

- 8.3 Unterbleibt die rechtzeitige Anzeige, ist der Auftragnehmer berechtigt, den durch die verspätete Anzeige verursachten Mehraufwand durch eine Schadenspauschale in Höhe von 50 % der monatlichen CardLink-Gebühr pro angefangener Woche der Verspätung, maximal iHv. drei monatlichen CardLink-Gebühr geltend zu machen. Dem Auftraggeber bleibt der Nachweis eines geringeren Schadens vorbehalten. Eine Zahlungspflicht für Leistungen, die nach dem tatsächlichen Vollzug des Inhaberwechsels nicht mehr durch den Auftraggeber in Anspruch genommen werden, wird hierdurch nicht begründet.
- 8.4 Der Auftraggeber sichert hiermit gegenüber dem Auftragnehmer zu, dass der neue Inhaber zum Erhalt personenbezogener Daten (einschließlich von Gesundheitsdaten) von Kunden des Auftraggebers berechtigt ist und der Auftraggeber hierfür alle erforderlichen Erklärungen oder Einwilligungen der betroffenen Kunden eingeholt hat, die ihn im Rahmen des Inhaberwechsels zu einer Übertragung ihrer personenbezogenen Daten berechtigen. Der Auftraggeber stellt den Auftragnehmer von sämtlichen Ansprüchen frei, die gegen den Auftragnehmer und/oder dessen Rechtsnachfolger(n) in Zusammenhang mit der vorstehend gemachten Zusicherung und/oder der Zurverfügungstellung der personenbezogenen Daten der Kunden des Auftraggebers geltend gemacht werden und haftet für dem Auftragnehmer und/oder dessen Rechtsnachfolger(n) hieraus entstehenden Schaden einschließlich der angemessenen Kosten der Rechtsverfolgung und -verteidigung.

9. Haftung

Es wird auf Artikel 82 DSGVO verwiesen. Im Übrigen richtet sich die Haftung aus diesem AVV nach der Vereinbarung.

10. Informationspflichten, Schriftformklausel, Rechtswahl

- 10.1 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 jeweilige Dritte (z. B. einen Gerichtsvollzieher) unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „Verantwortlicher“ im Sinne der DSGVO liegen.

- 10.2 Folgende Anhänge sind Bestandteil dieses AVV. Bei Widersprüchen gehen die Regelungen des Textes dieses AVV den Anhängen vor:

Annex 1: Angaben zur Verarbeitung

Annex 2: Liste und Kontaktdaten der Ansprechpartner

Annex 3: Liste genehmigter Unter-Auftragsverarbeiter

Annex 4: Technische und organisatorische Maßnahmen (TOM)

- 10.3 Für Änderungen und Ergänzungen dieser AVV gelten die Formvorschriften der Vereinbarung.
- 10.4 Bei Widersprüchen geht dieser AVV in seinem Anwendungsbereich den Regelungen der Vereinbarung vor.
- 10.5 Sollten einzelne Teile dieses AVV unwirksam sein, so berührt dies die Wirksamkeit des AVV im Übrigen nicht.
- 10.6 Auf diesen AVV findet das für die Vereinbarung geltende Recht Anwendung. Ausschließlicher Gerichtsstand ist der für die Vereinbarung vereinbarte Gerichtsstand.

Annex 1: Angaben zur Verarbeitung

Der Gegenstand der Auftragsverarbeitung ist in der Vereinbarung ausführlich beschrieben. Im Wesentlichen ist hiervon Folgendes umfasst:

1.1 Art und Zweck der Verarbeitung sind in der Vereinbarung konkretisiert und umfassen insbesondere:

Der Auftraggeber betreibt das entsprechende informationstechnische System. Der Auftragnehmer stellt einen Teil der hierfür notwendigen technischen Infrastruktur (u.a. Anbindung an CardLink-Verfahren und technisch notwendige Schnittstellen) zur Verfügung und verarbeitet in diesem Zusammenhang pbD im Auftrag des Auftraggebers, einschließlich von **Gesundheitsdaten**.

Die technischen Prozessschritte sind in der Vereinbarung beschrieben.

1.2 Die Verarbeitung betrifft die nachfolgend genannten Arten von Daten:

a) Personenbezogene Daten eines Versicherten. Entsprechende pbD sind üblicherweise:

- Alle Angaben des Versicherten auf dem Rezept des Versicherten (in der Regel: Vorname, Nachname, Alter, Versichertennummer, Krankenkasse, Medikation).
- **Gesundheitsdaten des Versicherten**
- Angaben zu der Person, die ein fremdes Rezept einlösen möchte.
- Kommunikationsdaten zur Einlösung von e-Verordnungen und zur Anzeige der Rezeptdaten in der gesund.de App (inkl. Daten, die bei der Nutzung der Near Field Communication- und der Card-Link-Communication-Lösung verarbeitet werden; Daten, die im Rahmen der Kommunikation mit einem Warenwirtschaftssystem verarbeitet werden; ggf. Standortdaten und/oder Auswahl einer konkreten Apotheke).
- Zuordnungsdaten, um verschlüsselte / pseudonymisierte Daten einem konkreten Versicherten zuordnen zu können.
- je nach Rechtsgrundlage: erweiterte Speicherung der Verordnungsdaten (inkl. Historie).

b) Personenbezogene Daten einer ausstellenden Person (z. B. Ärztin/Arzt). Entsprechende pbD sind üblicherweise:

- Alle Angaben der ausstellenden Person auf dem Rezept des Versicherten.
- Name, Anschrift, Telefonnummer und ggf. weitere Kontaktdaten der ausstellenden Person.

c) Personenbezogene Daten eines Mitarbeiters / einer Mitarbeiterin des Auftraggebers. Entsprechende pbD sind üblicherweise:

- Login-Daten für das informationstechnische Systems zur Entgegennahme von elektronischen Zugangsdaten zu einer e-Verordnung.

- Nutzungsdaten im Rahmen des informationstechnischen Systems zur Entgegennahme von elektronischen Zugangsdaten zu einer e-Verordnung.

1.3 Folgende Kategorien von betroffenen Personen sind von der Verarbeitung betroffen:

- a) Versicherte und Dritte, die ein fremdes Rezept einlösen.
- b) Ausstellende Personen (z. B. Ärztin/Arzt).
- c) Mitarbeiter und sonstige Berechtigte des Auftraggebers, zur Nutzung des informationstechnischen Systems e-Verordnung.

1.4 Laufzeit und Kündigungsrechte

Die AVV wird für die Laufzeit der Vereinbarung abgeschlossen. Eine Beendigung der Vereinbarung führt automatisch zur Beendigung dieser AVV. Eine Beendigung der AVV führt automatisch zur Beendigung der Vereinbarung.

1.5 Erlaubnis zur Datenübermittlungen an den Auftragnehmer / Datennutzung durch den Auftragnehmer für eigene Verarbeitungszwecke

Wenn ein Versicherter eine entsprechende Einwilligung gegenüber dem Auftragnehmer und/oder dem Auftraggeber abgibt, oder eine andere datenschutzrechtliche Rechtsgrundlage gegeben ist, erlaubt der Auftraggeber dem Auftragnehmer eine Datenübermittlung / Datennutzung der pbD, einschließlich der **Gesundheitsdaten**, auch für eigene Zwecke (insb. zur Übermittlung an eigene IT-Systeme zur Anzeige der Rezeptdaten in der gesund.de App; inklusive der jeweiligen Historie im Einzelfall).

Annex 2: Liste und Kontaktdaten der Ansprechpartner

Die Kontaktdaten der Ansprechpartner ergeben sich aus der Vereinbarung.

Weisungsempfänger beim Auftragnehmer sind:

Name	Telefon	E-Mail
Martin Mathlouthi	+49 171 7840206	Martin.Mathlouthi@gesund.de

Der Datenschutzbeauftragte beim Auftragnehmer ist:

Kontaktinformationen	E-Mail
Sie finden die aktuellen Kontaktinformationen hier: https://www.gesund.de/datenschutz	datenschutz@gesund.de.

Bei einem Wechsel oder einer längerfristigen Verhinderung eines Ansprechpartners wird der Auftragnehmer Kontaktdaten eines Nachfolgers/Vertreters veröffentlichen.

Annex 3: Liste genehmigter Unter-Auftragsverarbeiter

Der Auftragnehmer setzt folgende Unter-Auftragsverarbeiter ein:

Service	Einsatzzweck	Name	Verarbeitung von personenbezogenen Daten	Rechtsgrundlage für int. Datenübermittlung (falls relevant)
N-Connect-Hub	Anbindung der gesund.de Plattform an die von der NGDA entwickelte und betriebene Datenaustauschplattform N-Connect-Hub und deren Nutzung.	NGDA - Netzgesellschaft Deutscher Apotheker mbH Carl-Mannich-Straße 26 65760 Eschborn	Alle in Annex 1 / 1.2. / a) und b) genannten pbD eines Versicherten / einer ausstellenden Person.	Keine int. Datenübermittlung geplant.
Card-Link	Bereitstellung des eHealth-CardLink-Verfahrens und Support.	Akquinet	Alle in Annex 1 / 1.2. / a) und b) genannten pbD eines Versicherten / einer ausstellenden Person.	Keine int. Datenübermittlung geplant.

Annex 4: Technische und organisatorische Maßnahmen (TOM)

Sie finden die entsprechenden TOM zum Card-Link-Verfahren in Ihrem Apotheken-Cockpit.
