Anlage 1 zu den Nutzungsbedingungen des GEDISA ApothekenPortals: Auftragsverarbeitungsvertrag („AVV“)

§ 1 Gegenstand und Dauer des Auftrags

(1) Die GEDISA mbH (im Folgenden „**Auftragnehmerin**“) führt die in den Nutzungsbedingungen des GEDISA ApothekenPortals beschriebenen Dienstleistungen für die leistungsbeziehende Apotheke (im Folgenden „**Auftraggeberin**“) durch. Konkreter Gegenstand, Art und Zweck der Verarbeitung, die Art der Daten sowie die Kategorien betroffener Personen sind dort beschrieben und werden durch den Anhang 1 dieser Vereinbarung ergänzt.

(2) Diese Vereinbarung tritt durch das Bereitstellen der von der Auftraggeberin ausgewählten Dienstleistungen und den Abschluss des diesbezüglichen Vertrages durch die Auftraggeberin in Kraft und gilt solange, wie der übergeordnete Hauptvertrag gilt und die Auftragnehmerin für die Auftraggeberin personenbezogene Daten verarbeitet.

§ 2 Weisungen der Auftraggeberin

(1) Die Auftraggeberin ist für die Einhaltung der gesetzlichen Bestimmungen des Datenschutzrechts, insbesondere für die Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Betroffenenrechte verantwortlich. Gesetzliche oder vertragliche Haftungsregelungen bleiben hiervon unberührt.

(2) Die Auftragnehmerin verarbeitet die ihr zur Verfügung gestellten personenbezogenen Daten ausschließlich nach den Weisungen der Auftraggeberin und im Rahmen der getroffenen Vereinbarungen. Daten dürfen nur berichtigt, gelöscht und gesperrt werden, wenn die Auftraggeberin dies anweist.

(3) Die Verarbeitung erfolgt nur auf Weisung der Auftraggeberin, es sei denn, die Auftragnehmerin ist durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem die Auftragnehmerin unterliegt, zur Verarbeitung dieser Daten verpflichtet. In einem solchen Fall teilt die Auftragnehmerin der Auftraggeberin diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine Mitteilung nicht wegen eines wichtigen öffentlichen Interesses untersagt.

(4) Weisungen sind nur schriftlich oder in Textform zu erteilen.

(5) Ist die Auftragnehmerin der Ansicht, dass eine Weisung der Auftraggeberin gegen datenschutzrechtliche Vorschriften verstößt, hat sie die Auftraggeberin unverzüglich darauf hinzuweisen. Die Auftragnehmerin ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch die Auftraggeberin bestätigt oder geändert wird.

§ 3 Technische und organisatorische Maßnahmen

(1) Die Auftragnehmerin verpflichtet sich, für die zu verarbeitenden Daten angemessene technische und organisatorische Sicherheitsmaßnahmen zu treffen und diese im **Anhang 3** dieser Vereinbarung zu dokumentieren. Die Sicherheitsmaßnahmen haben ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

(2) Die getroffenen Maßnahmen können im Laufe der Zeit der technischen und organisatorischen Weiterentwicklung angepasst werden. Die Auftragnehmerin darf entsprechende Anpassungen nur vornehmen, wenn diese mindestens das Sicherheitsniveau der bisherigen Maßnahmen erreichen. Soweit nichts anderes bestimmt ist, muss die Auftragnehmerin der Auftraggeberin nur wesentliche Anpassungen mitteilen.

(3) Die Auftragnehmerin unterstützt die Auftraggeberin bei der Einhaltung der gesetzlichen Pflichten hinsichtlich der einzuhaltenden technischen und organisatorischen Maßnahmen. Sie hat der Auftraggeberin alle erforderlichen Angaben und Dokumente auf Anfrage offenzulegen.

§ 4 Pflichten der Auftragnehmerin

(1) Die Auftragnehmerin bestätigt, dass ihr die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Sie gestaltet in ihrem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

(2) Die Auftragnehmerin bietet hinreichende Garantien dafür, dass die geeigneten technischen und organisatorischen Maßnahmen durchgeführt werden, die gewährleisten, dass die Verarbeitung im Einklang mit den datenschutzrechtlichen Vorschriften und den Rechten der betroffenen Person steht.

(3) Die Auftragnehmerin sichert zu, dass sie die bei der Durchführung der Arbeiten beschäftigten Personen mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. **Die Beschäftigten der Auftragnehmerin sind darüber hinaus als Mitwirkende zur Verschwiegenheit nach § 203 StGB verpflichtet**, soweit sie auf personenbezogene Daten der Kundinnen und Kunden der Auftraggeberin zugreifen, die dem Apothekergeheimnis unterliegen. Die Auftragnehmerin überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.

(4) Die Auftragnehmerin darf im Rahmen der Auftragsverarbeitung nur dann auf personenbezogene Daten der Auftraggeberin zugreifen, wenn dies für die Durchführung der Auftragsverarbeitung zwingend erforderlich ist.

(5) Soweit gesetzlich vorgeschrieben, bestellt die Auftragnehmerin einen Beauftragten für den Datenschutz. Die Kontaktdaten des Beauftragten für den Datenschutz werden der Auftraggeberin zum Zweck der direkten Kontaktaufnahme in **Anhang 1** mitgeteilt.

(6) Die Auftragnehmerin darf die ihr zur Verfügung gestellten personenbezogenen Daten ausschließlich im Gebiet der Bundesrepublik Deutschland oder in einem Mitgliedsstaat der Europäischen Union verarbeiten. Die Verarbeitung von personenbezogenen Daten in einem Drittland bedarf stets der vorherigen schriftlichen Zustimmung der Auftraggeberin und darf nur erfolgen, wenn die besonderen gesetzlichen Voraussetzungen erfüllt sind.

(7) Die Auftragnehmerin unterstützt die Auftraggeberin mit geeigneten technischen und organisatorischen Maßnahmen, damit diese ihre bestehenden Pflichten gegenüber der betroffenen Person erfüllen kann, z. B. die Information und Auskunft an die betroffene Person, die Berichtigung oder Löschung von Daten, die Einschränkung der Verarbeitung oder das Recht auf Datenübertragbarkeit und Widerspruch. Die Auftragnehmerin benennt einen Ansprechpartner, der die Auftraggeberin bei der Erfüllung von gesetzlichen Informations- und Auskunftspflichten, die im Zusammenhang mit der Auftragsverarbeitung entstehen, unterstützt und teilt der Auftraggeberin dessen Kontaktdaten unverzüglich mit. Soweit die Auftraggeberin besonderen gesetzlichen Informationspflichten bei unrechtmäßiger Kenntniserlangung von Daten unterliegt, unterstützt die Auftragnehmerin die Auftraggeberin hierbei. Auskünfte an die betroffene Person oder Dritte darf die Auftragnehmerin nur nach vorheriger Weisung der Auftraggeberin erteilen. Soweit eine betroffene Person ihre datenschutzrechtlichen Rechte unmittelbar gegenüber der Auftragnehmerin geltend macht, wird die Auftragnehmerin dieses Ersuchen unverzüglich an die Auftraggeberin weiterleiten.

(8) Die Auftragnehmerin unterstützt die Auftraggeberin bei der Erfüllung ihrer Pflicht zur Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Anforderungen.

§ 5 Fernzugriff zur Prüfung, Wartung oder Fehlerbehebung

(1) Für die Durchführung von sogenannten Fernzugriffen zu Prüfungs- oder Wartungszwecken bzw. zur Fehlerbehebung auf Datenverarbeitungsanlagen durch die Auftragnehmerin ("Remote Access-Maßnahmen"), z.B. auf Rechner oder Systeme der Auftraggeberin gilt:

a. Remote Access-Maßnahmen an Systemen werden erst nach Freigabe der Auftraggeberin bzw. Ihrer Mitarbeiter, z.B. durch Anklicken einer Pop-Up-Box auf dem Rechner, durchgeführt.

b. Remote Access-Maßnahmen an automatisierten Verfahren oder Datenverarbeitungsanlagen werden, sofern hierbei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann, grundsätzlich, soweit z.B. nicht Gefahr im Verzug ist, nur mit Zustimmung der Auftraggeberin ausgeführt.

c. Falls notwendig werden sich Auftragnehmerin und Auftraggeberin vor Durchführung von Remote Access-Maßnahmen über etwaig notwendige Datensicherungsmaßnahmen in ihrem jeweiligen Verantwortungsbereich verständigen.

d. Die Auftragnehmerin verwendet angemessene Identifizierungs- und Verschlüsselungsverfahren und wird von den eingeräumten Zugriffsrechten nur in dem Umfang Gebrauch machen, wie dies für die ordnungsgemäße Durchführung der Remote Access-Maßnahme notwendig ist.

e. Remote Access-Maßnahmen werden dokumentiert und protokolliert. Die Auftraggeberin ist soweit technisch möglich berechtigt, die Remote Access-Maßnahmen vor, während und nach Durchführung zu verfolgen, zu kontrollieren und jederzeit abzubrechen.

f. Soweit eine Fehleranalyse erforderlich ist, die eine Kenntnisnahme (z.B. lesender Zugriff) oder einen Zugriff auf oder einen Abzug von Produktivbetriebsdaten (Produktions-/Echtdaten) der Auftraggeberin notwendig macht, wird die Auftragnehmerin die Zustimmung einholen. Bei Datenabzug wird die Auftragnehmerin alle Kopien nach Bereinigung des Fehlers vom verwendeten Speichermedium löschen. Produktivbetriebsdaten dürfen nur zum Zweck der Fehleranalyse verarbeitet werden.

g. Remote Access-Maßnahmen sowie sämtliche in diesem Zusammenhang erforderlichen Tätigkeiten, insbesondere Tätigkeiten wie Löschen, Datentransfer oder eine Fehleranalyse, werden unter Berücksichtigung der in Anhang 3 genannten TOM durchgeführt.

§ 6 Berechtigung zur Begründung von Unterauftragsverhältnissen

(1) Die Auftragnehmerin darf Unterauftragnehmer nur beauftragen, wenn sie die Auftraggeberin über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter informiert, wodurch die Auftraggeberin die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Der Einspruch darf nur aus wichtigem Grund erfolgen und muss binnen 14 Tagen ab Information erfolgen.

(2) Unabhängig davon darf die Auftragnehmerin Unterauftragnehmer in Drittländern außerhalb der Europäischen Union („EU“) bzw. des Europäischen Wirtschaftsraums („EWR“) nur beauftragen, wenn die Auftraggeberin dies vorher schriftlich genehmigt hat.

(3) Ein Unterauftragsverhältnis liegt insbesondere vor, wenn die Auftragnehmerin weitere Auftragnehmer in Teilen oder im Ganzen mit Leistungen beauftragt, auf die sich der Hauptvertrag bezieht. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die die Auftragnehmerin bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z. B. Telekommunikationsleistungen oder Reinigungskräfte. Die Auftragnehmerin ist jedoch verpflichtet, zur Gewährleistung des Schutzes

und der Sicherheit der Daten der Auftraggeberin auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(4) Ein Zugriff auf Daten darf durch den Unterauftragnehmer erst dann erfolgen, wenn die Auftragnehmerin durch einen schriftlichen Vertrag sicherstellt, dass die in dieser Vereinbarung getroffenen Regelungen auch gegenüber den Unterauftragnehmern gelten, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den datenschutzrechtlichen Vorschriften erfolgt. **Dies beinhaltet auch, dass die Beschäftigten des Unterauftragnehmers, soweit sie auf personenbezogene Daten der Kundinnen und Kunden der Auftraggeberin zugreifen, die dem Apothekergeheimnis unterliegen, als Mitwirkende zur Verschwiegenheit nach § 203 StGB verpflichtet werden.**

(5) Die Inanspruchnahme der in **Anhang 2** zum Zeitpunkt der Vertragsunterzeichnung aufgeführten Unterauftragnehmer gilt als genehmigt.

§ 7 Kontrollrechte der Auftraggeberin

(1) Die Auftragnehmerin erklärt sich damit einverstanden, dass die Auftraggeberin oder eine von ihr beauftragte Person berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften und Anforderung von relevanten Unterlagen, die Einsichtnahme in die Verarbeitungsprogramme oder durch Zutritt zu den Arbeitsräumen der Auftragnehmerin zu den ausgewiesenen Geschäftszeiten nach vorheriger Anmeldung. Durch geeignete und gültige Zertifikate zur IT-Sicherheit (z. B. IT-Grundschutz, ISO 27001) kann auch der Nachweis einer ordnungsgemäßen Verarbeitung erbracht werden, sofern hierzu auch der jeweilige Gegenstand der Zertifizierung auf die Auftragsverarbeitung im konkreten Fall zutrifft. Die Vorlage eines relevanten Zertifikats ersetzt jedoch nicht die Pflicht der Auftragnehmerin zur Dokumentation der Sicherheitsmaßnahmen im Sinne des § 3 dieser Vereinbarung.

(2) Beauftragt die Auftraggeberin Dritte mit der Durchführung, so hat die Auftraggeberin den Dritten schriftlich auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen der Auftragnehmerin hat die Auftraggeberin diese Verpflichtungsvereinbarungen unverzüglich vorzulegen. Die Auftraggeberin darf keinen Wettbewerber der Auftragnehmerin mit der Kontrolle beauftragen.

§ 8 Mitzuteilende Verstöße der Auftragnehmerin

(1) Die Auftragnehmerin unterrichtet die Auftraggeberin unverzüglich über Störungen des Betriebsablaufs, die Gefahren für die Daten der Auftraggeberin mit sich bringen, sowie bei Verdacht auf Datenschutzverletzungen im Zusammenhang mit den Daten der Auftraggeberin. Gleiches gilt, wenn die Auftragnehmerin feststellt, dass die bei ihr getroffenen Sicherheitsmaßnahmen den gesetzlichen Anforderungen nicht genügen. Der Auftragnehmerin ist bekannt, dass die Auftraggeberin verpflichtet ist, umfassend alle Verletzungen des Schutzes personenbezogener Daten zu dokumentieren und ggf. den Aufsichtsbehörden bzw. der betroffenen Person unverzüglich zu melden. Sofern es zu solchen Verletzungen gekommen ist, wird die Auftragnehmerin die Auftraggeberin bei der Einhaltung ihrer Meldepflichten unterstützen. Sie wird die Verletzungen der Auftraggeberin unverzüglich melden und hierbei zumindest folgende Informationen mitteilen:

   (a) eine Beschreibung der Art der Verletzung, der Kategorien und ungefähre Anzahl der betroffenen Personen und Datensätze,

(b) Name und Kontaktdaten eines Ansprechpartners für weitere Informationen,

(c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung, sowie

(d) eine Beschreibung der ergriffenen Maßnahmen zur Behebung oder Abmilderung der Verletzung.

§ 9 Anonymisierungsvereinbarung

(1) Die Auftragnehmerin hat das Recht, die von dieser Vereinbarung umfassten personenbezogenen Daten zu anonymisieren und vorher die für die Anonymisierung erforderlichen Verarbeitungsschritte durchzuführen. Unter Wahrung der Anonymität kann die Auftragnehmerin alle so entstandenen Daten für statistische Auswertungen und vergleichbare Zwecke verarbeiten und nutzen. Der ursprüngliche Datenbestand ist von dieser Anonymisierung nicht betroffen und wird strikt getrennt.

§ 10 Haftung

(1) Bezüglich der Haftung der Auftragnehmerin gelten die Bestimmungen der vereinbarten Nutzungsbedingungen.

§ 11 Beendigung des Auftrags

(1) Nach Abschluss der Auftragsverarbeitung hat die Auftragnehmerin alle personenbezogenen Daten nach Wahl der Auftraggeberin entweder zu löschen oder zurückzugeben, soweit nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

(2) Beide Parteien können das Auftragsverhältnis ohne Einhaltung einer Frist kündigen, wenn die jeweils andere Partei einen schwerwiegenden Verstoß gegen die Bestimmungen dieses Vertrags oder gegen datenschutzrechtliche Bestimmungen begeht und aufgrund dessen die Fortsetzung der Auftragsverarbeitung bis zum Ablauf der Kündigungsfrist des Hauptvertrags (Ziffer 7 ff. der Nutzungsbedingungen des GEDISA ApothekenPortals) oder bis zu der vereinbarten Beendigung des Auftrags nicht zugemutet werden kann. Mit der Kündigung des Auftragsverarbeitungsverhältnisses erlischt gleichzeitig der Anspruch zur Nutzung des GEDISA ApothekenPortals.

§ 12 Schlussbestimmungen

(1) Sollte das Eigentum der Auftraggeberin bei der Auftragnehmerin durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat die Auftragnehmerin die Auftraggeberin unverzüglich zu verständigen. Ein Zurückbehaltungsrecht ist in Bezug auf Datenträger und Datenbestände der Auftraggeberin ausgeschlossen.

(2) Sollten einzelne Teile dieses Vertrags unwirksam sein, so berührt dies die Wirksamkeit des Vertrags im Übrigen nicht.

Anhang 1 zur Vereinbarung über die Auftragsverarbeitung

Gegenstand, Art und Zweck der Verarbeitung, Datenkategorien, betroffene Personen, Kontaktdaten der Datenschutzbeauftragten

Gegenstand der Verarbeitung	Die Verarbeitung personenbezogener Daten und besonderer Kategorien personenbezogener Daten erfolgt im Rahmen der Bereitstellung von Portalfunktionen für die Apotheke und beinhaltet gegenwärtig die folgenden Funktionalitäten: 1. Die Auftraggeberin kann in der Anwendung zur Impfsurveillance gem. § 4 Corona-Impfverordnung die benötigten Patientendaten eintragen und an das RobertKoch-Institut übermitteln. 2. Die Auftraggeberin kann in der Anwendung zur Impfsurveillance gem. § 13 Absatz 5 Satz 1 des Infektionsschutzgesetzes die benötigen Patientendaten eintragen und an das Robert-Koch-Institut übermitteln. 3. Weiterhin kann die Auftraggeberin in der Anwendung zur Impfsurveillance gem. § 35a ApoBetrO die benötigten Patienten- und Apothekendaten erfassen und in ausgedruckter Form zu Dokumentationszwecken zur Verfügung stellen. 4. Die Auftragnehmerin stellt für die Anwendung "Terminbuchungen", die durch APOMONDO GmbH zur Verfügung gestellt wird, im Apothekenportal einen Absprungpunkt zur Verfügung. Personenbezogene Patientendaten werden in diesem Zusammenhang durch die Auftragnehmerin nicht verarbeitet. 5. Ferner werden Daten für die Abrechnung von telepharmazeutischen Dienstleistungen sowie von Impfungen gegen das Coronavirus und das Grippevirus verarbeitet. 6. Des Weiteren werden pseudonymisierte Daten für statistische Datenerhebung zu eigenen Zwecken der Auftragnehmerin verarbeitet. 7. In der Anwendung können Mitarbeiterlogins angelegt werden. 8. Chat (Ende-zu-Ende-Verschlüsselung) zur internen (innerhalb eines Filialverbundes) Kommunikation: 9. Chat (Ende-zu-Ende-Verschlüsselung) zur Kommunikation mit Patienten: In dieser Anwendung können Mitarbeiterkonten angelegt werden. 10. Pharmazeutische Dienstleistungen (pDL): die Auftraggeberin kann in der Anwendung pDL gem. VorOrt-Stärkungsgesetz (VOASG) und § 129 Abs. 5e SGB V Patientendaten eintragen und verarbeiten. 11. Die Auftragnehmerin stellt für das Anmelde-/Authentifizierungsverfahren einen IDP zur Verfügung, der durch die Firma Research Industrial Systems Engineering (RISE) Forschungs-, Entwicklungs- und Großprojektberatung GmbH betrieben wird. In dieser Anwendung können Mitarbeiterkonten angelegt werden. Personenbezogene Patientendaten werden in diesem Zusammenhang durch die Auftragnehmerin nicht verarbeitet.

	12. Die Auftragnehmerin stellt einen E-Mail-Service bereit, der durch die Smaser AG zur Verfügung gestellt wird. In dieser Anwendung können Inhaber- und Mitarbeiterkonten angelegt werden. 13. Die Auftragnehmerin stellt einen Bestellprozess für ApoGuide-Werbemittel zur Verfügung. Die gesamte Abwicklung der ApoGuide Werbemittel inklusive Bestellung und Versand erfolgt über unseren Vertragspartner reprogress GmbH. 14. Die Auftragnehmerin stellt KIM-Adressen zum Zwecke des Informationsaustauschs mit Leistungserbringern des Gesundheitswesens bereit. Die Bereitstellung erfolgt durch die akquinet health service GmbH, die den KIM-Fachdienst betreibt. 15. Durchführung von Remote Access-Maßnahmen zwecks Prüfung, Wartung oder zur Fehlerbehebung 16. Bereitstellung eines sicheren Datenraums
Art und Zweck der Verarbeitung	1. Eingabe und Übermittlung von Patientendaten an das RKI zur Erfüllung der Pflicht zur Grippe Impfsurveillance gem. § 13 Absatz 5 Satz 1 des Infektionsschutzgesetzes. 2. Eingabe von Patientendaten und Apothekendaten zur Erfüllung der Dokumentationspflicht gem. § 35a ApoBetrO. 3. Übermittlung der Apothekendaten (Name, Anschrift, E-Mail, Telefonnummer, Telefax, Anschrift) sowie des Nutzernamens an die APOMONDO GmbH zur Bereitstellung des Terminbuchungsservices. 4. Zurverfügungstellung von Daten für die Abrechnung von Impfungen gegen das Corona- und das Grippevirus durch Apotheken 5. Zurverfügungstellung von Daten für statistische Datenerhebung zu eigenen Zwecken der Auftragnehmerin 6. Erstellung von Mitarbeiterlogins (Nutzungsberechtigte) zur gleichzeitigen Ausstellung mehrerer Zertifikate in der Apotheke 7. Erfassen und Zurverfügungstellung von Patientendaten zum Zweck der Terminvereinbarung in der Apotheke 8. Erstellung von Mitarbeiterlogins (Bearbeiterin) zur Nutzung der Chatfunktion zum Zweck der internen Kommunikation innerhalb eines Filialverbundes und zur Kommunikation mit Patient*innen 9. Erfassen und Zurverfügungstellung von Patienten- und Apothekendaten (Bearbeiterin) zur Beratung, Aufklärung und Dokumentation von pDL 10. Erstellung von Mitarbeiteraccounts zur Nutzung der bereitgestellten Dienstleistungen des GEDISA ApothekenPortals 11. Erstellung von Inhaber-/Mitarbeiterlogins zur Nutzung des E-Mail-Service für die innerbetriebliche Kommunikation in der Apotheke 12. Erstellung von Mitarbeiterlogins zur Nutzung des E-Mail-Services zu folgenden Zwecken: a. Anmeldung am IDP b. Passwort Reset für das GEDISA ApothekenPortal c. Allgemeine Kommunikation zwischen Apotheke Dritten, aber nicht zur Kommunikation von besonderen Kategorien personenbezogener Daten im Sinne von Art.9 DSGVO –

	insbesondere nicht zur Kommunikation über personenbezogene Gesundheitsdaten der Kundinnen und Kunden der Apotheke 13. Im Rahmen der Bestellübermittlung (für kostenfreie ApoGuide Werbemittel) an die Firma reprogress GmbH werden personenbezogenen Daten der Inhaberin/des Inhabers und die Apothekendaten verarbeitet. 14. Erheben, Kopieren, Löschen, Auswerten sowie die Durchführung aller weiteren Datenverarbeitungen, die im Rahmen von Remote Access-Maßnahmen zur Fehlerbehebung erforderlich sind.
Art der personenbezogenen Daten	1. Name, Vorname und Geburtsdatum des/der Patient*in, Versicherungsstatus, Versichertennummer, Zugehörigkeit STIKO Empfehlungsgruppe, Information zum Impfstoff, Information zur Impfung bzw. zum Genesenenstatus und einem damit verbundenen positiven Corona-Testergebnis, 2. Patienten-Pseudonym, Geburtsmonat und -jahr, Geschlecht, PLZ und Landkreis der Patient*in, Kennnummer und Landkreis der Apotheke, Datum der Impfung, Beginn oder Abschluss der Impfserie (Erst-, Folge-, Auffrischimpfung), impfstoffspezifische Dokumentationsnummer, Chargennummer 3. Anamnesedaten 4. Anrede, Titel, Namenszusatz, Namen, Geschlecht und Kontaktdaten der ausgewählten Mitarbeiterinnen und Mitarbeiter 5. Name der Apotheke, Vorname und Nachname der Inhaberin/des Inhabers, Adresse der Apotheke
Kategorien betroffener Personen	1. Kundinnen und Kunden der Auftraggeberin 2. Mitarbeiterinnen und Mitarbeiter der Auftraggeberin 3. Inhaberin der Auftraggeberin
Datenschutzbeauftragter der Auftragnehmerin (sofern benannt)	RA Patricia Kühnel datenschutzbeauftragte@gedisa.de Telefon: 03362/9380705

Anhang 2 zur Vereinbarung über die Auftragsverarbeitung

Liste der beauftragten Unterauftragnehmer einschließlich der Verarbeitungsstandorte

Unterauftragnehmer Name, Rechtsform, Sitz der Gesellschaft	Verarbeitungsstandort	Art der Dienstleistung
abilita GmbH	Prüfeninger Straße 20, 93049 Regensburg, Deutschland	Rechnungsversand, Durchführung des Mahnwesens, Bereitstellung von Reports zu erbrachten Leistungen
akquinet health service GmbH Paul-Stritter-Weg 5 22297 Hamburg	Deutschland	Entwicklungs-, Implementierungs- und Betriebspartner für Kommunikation im Medizinwesen („KIM“) und CardLink
APOMONDO Gmbh Rennweg 54 90768 Fürth	Deutschland	Entwicklung und Betrieb der Funktion Terminverwaltung
Cyrano Kommunikations GmbH Hohenzollernring 49-51 48145 Münster	Deutschland	Hosting
famedly GmbH Prenzlauer Allee 221 10405 Berlin	Deutschland	Entwicklungs-, Implementierungs- und Betriebspartner für den Chat
Hetzner Online GmbH Industriestr. 25 91710 Gunzenhausen	Deutschland	Infrastruktur-Hosting
reprogress GmbH Chemnitzer Strasse 46b 01187 Dresden	Deutschland	Marketing, Versanddienstleistungen
Research Industrial Systems Engineering (RISE) Forschungs-, Entwicklungs- und Großprojektberatung GmbH FN 280353i (LG Korneuburg) Concorde Business Park F 2320 Schwechat Österreich	Deutschland	Entwicklung und Betrieb des Identity Providers („IDP“)
DVG Operations GmbH Hilpertstraße 20, 64295 Darmstadt Germany	Deutschland	Infrastruktur-Hosting, Entwicklung und Betrieb Service Desk

Imtercolo GmbH Carl-Goerdler-Straße 114, 60320 Frankfurt am Main, Deutschland	Deutschland	Hosting verschlüsselter Backups

Anhang 3 zur Vereinbarung über die Auftragsverarbeitung

Technische und organisatorische Maßnahmen zur Wahrung des Datenschutzes

Um ein ausreichendes Schutzniveau für verarbeitete personenbezogenen Daten zu gewährleisten, hat die GEDISA zahlreiche technische und organisatorische Maßnahmen umgesetzt. Diese setzt die GEDISA selbst um oder hat die Verpflichtung zur Umsetzung an ihre Unterauftragnehmer übertragen, soweit es im Kontext der verarbeiteten Daten notwendig ist.

Die nachfolgende Übersicht gemäß Art.32 DSGVO bezieht sich auf die Bereitstellung des GEDISA ApothekenPortals sowie die damit verbundenen weiteren Services.

Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle

Folgende Maßnahmen sind umgesetzt, um Unbefugten der Zutritt zu Datenverarbeitungsanlagen, auf denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Technische Maßnahmen	Organisatorische Maßnahmen
• Manuelles Schließsystem	• Schlüsselregelung (Schlüsselausgabe etc.)
• Absicherung von Gebäudeschächten	• Mitarbeiter- und Berechtigungsausweise
• Videoüberwachung	• Sperrbereiche
• Sicherheitsschlösser, Sicherheitstüren / -fenster	• Besucherregelung
• Personenkontrolle beim Pförtner/Empfang	•
• Sorgfältige Auswahl von Reinigungspersonal	•
• Zutrittskontrollsystem, Ausweisleser (Magnet-/Chipkarte)	•
• Türsicherungen (elektrische Türöffner, Zahlenschloss, etc.), Gitter vor Fenstern/Türen	•
• Werkschutz, Pförtner	•
• Alarmanlage	•
• Spezielle Schutzvorkehrungen des Serverraums	•
• Spezielle Schutzvorkehrungen für die Aufbewahrung von Backups und sonstigen Datenträgern	•
• Protokollierung des Zugangs	•

Zugangskontrolle

Folgende Maßnahmen sind umgesetzt, um die Nutzung personenbezogener Daten durch Unbefugte zu verhindern.

Technische Maßnahmen	Organisatorische Maßnahmen
• Zuordnung von Benutzerrechten	• Autorisierungsprozess für Zugangsberechtigungen
• Erstellen von Benutzerprofilen	• Kennwortrichtlinie
• Passwortvergabe	• Elektronische Dokumentation von Passwörtern und Schutz dieser Dokumentation vor unbefugtem Zugriff
• Authentifikation mit Benutzername/Passwort	• Maßnahmen zur Verhinderung unbefugten Überspielens von Daten auf extern verwendbare Datenträger
• Zuordnung von Benutzerprofilen zu IT-Systemen	• Funktionstrennung
• Einsatz von Anti-Viren-Software	•
• Einsatz von Hardware-Firewalls	•
• Einsatz von Software-Firewalls	•
• Zusätzlicher System-Log-In für bestimmte Anwendungen	•
• Verschlüsselung von Datenträgern	•
•	•

Zugriffskontrolle

Folgende Maßnahmen sind umgesetzt, damit Berechtigte ausschließlich auf diejenigen Daten zugreifen können, die ihrer Zugriffsberechtigung unterliegen und nach denen personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt, gelesen, kopiert, verändert oder entfernt werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
• Verwaltung der Rechte durch Systemadministratoren	• Anzahl der Administratoren auf das „Notwendigste" reduziert
• physische Löschung von Datenträgern vor Wiederverwendung, bzw. ordnungsgemäße Vernichtung von Datenträgern (z.B. nach DIN 32757)	• Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
• Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)	• Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
• Nicht-reversible Vernichtung von Datenträgern	• Sichere Aufbewahrung von Datenträgern
• Mobile Device Management-System	• Umsetzung eines Berechtigungskonzepts

Technische Maßnahmen	Organisatorische Maßnahmen
• Fachkundige Akten- und Datenträgervernichtung gemäß DIN 66399	• Verwaltung und Dokumentation von differenzierten Berechtigungen
•	• Autorisierungsprozess für Berechtigungen
•	• Vier-Augen-Prinzip

Protokollierung der Vernichtung

Folgende Maßnahmen sind umgesetzt, um die Vernichtung oder Löschung von Datenträgern zu dokumentieren

Technische Maßnahmen	Organisatorische Maßnahmen
•	• Protokollierung der Datenträgervernichtung

Trennungskontrolle

Folgende Maßnahmen sind umgesetzt, damit für unterschiedliche Zwecke erhobene Daten getrennt verarbeitet werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
• Logische Mandantentrennung (softwareseitig)	• Erstellung eines Berechtigungskonzepts
• Versehen der Datensätze mit Zweckattributen/Datenfeldern	• Zugriffsberechtigungen nach funktioneller Zuständigkeit
• Festlegung von Datenbankrechten	• Getrennte Datenverarbeitung durch differenzierende Zugriffsregelungen
• Trennung von Produktiv- und Testsystem	• Mandantenfähigkeit von IT-Systemen
• Verwendung von Testdaten	•
• Trennung von Entwicklungs- und Produktionsumgebung	•

Pseudonymisierung

Folgende Maßnahmen sind umgesetzt, um eine starke Pseudonymisierung von personenbezogener Daten zu gewährleisten, so dass sie ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer betroffenen Person zugeordnet werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
• Vergabe von Pseudonymen für weitere interne Verarbeitung	•
• Verschlüsselungsmaßnahmen i.S. einer Inhaltsverschlüsselung	•

Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle

Folgende Maßnahmen sind umgesetzt, damit während des Transports von personenbezogenen Daten diese nicht von Unbefugten gelesen, kopiert, verändert oder entfernt werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
• Beim physischen Transport: sichere Transportbehälter/-verpackungen	• Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
• Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und Transportfahrzeugen	• Fernwartungskonzept (z.B. Verschlüsselung, Ereignisauslösung durch Auftraggeber, Challenge-Response, Rückrufautomatik, Einmal-Passwort)
• Verschlüsselung des Speichermediums von Laptops	• Mobile Device Management-System
• Gesicherter File Transfer/Datentransport	• Regelung zum Umgang mit mobilen Speichermedien
• Gesichertes WLAN	•
• Data Loss Prevention (DLP)-System	•
• Protokollierung des Kopierens, Veränderns oder Entfernens von Daten	•
• Protokollierung von Datenübertragung oder Datentransport	•

Eingabekontrolle

Folgende Maßnahmen sind umgesetzt, damit nachträglich überprüft werden kann, ob, von wem und wann personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt wurden.

Technische Maßnahmen	Organisatorische Maßnahmen
• Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)	• Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können
• Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts	• Funktionelle Verantwortlichkeiten, organisatorisch festgelegte Zuständigkeiten
• Protokollierung der Eingabe, Änderung und Löschung von Daten	• Mehraugenprinzip
• Dokumenten Management System (DMS) mit Änderungshistorie	•

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Verfügbarkeitskontrolle

Folgende Maßnahmen gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Technische Maßnahmen	Organisatorische Maßnahmen
• Unterbrechungsfreie Stromversorgung (USV)	• Erstellen eines Backup- & Recovery-Konzepts
• Klimaanlage in Serverräumen	• Testen von Datenwiederherstellung
• Schutzsteckdosenleisten in Serverräumen	• Erstellen eines Notfallplans
• Feuer- und Rauchmeldeanlagen	• Sicherheitskonzept für Software- und IT-Anwendungen
• Feuerlöschgeräte in Serverräumen	• Aufbewahrungsregelungen für Backups
• Serverräume nicht unter sanitären Anlagen	• Redundante, örtlich getrennte Datenaufbewahrung (Offsite Storage)
• Datensicherungsverfahren	• Erfolgreiche Notfallübungen
• Bedarfsgerechtes Einspielen von Sicherheits-Updates	•
• Brand- und/oder Löschwasserschutz des Serverraums	•
• Firewall	•
• Virenschutz	•

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32. Abs. 1 lit. d) DSGVO)

Folgende Maßnahmen sind umgesetzt, damit die Maßnahmen zum Schutz personenbezogener Daten regelmäßig überprüft und bewertet werden. Das umfasst auch die Verarbeitung von personenbezogenen Daten durch Unterauftragnehmer entsprechend den Weisungen des Verantwortlichen werden.

Datenschutz-Management

Folgende Maßnahmen gewährleisten, dass das Datenschutzmanagementsystem den Bedarfen entspricht und rechtliche Vorgaben berücksichtigt.

Technische Maßnahmen	Organisatorische Maßnahmen
•	• Datenschutzleitbild
•	• Datenschutz-Richtlinie
•	• Richtlinien/Anweisungen zur Gewährleistung von technisch-organisatorischen Maßnahmen zur Datensicherheit
•	• Auftragnehmer hat Datenschutzbeauftragten bestellt
•	• Verpflichtung der Mitarbeiter auf Verschwiegenheit / Berufsgeheimnis
•	• Schulungen der Mitarbeiter in Datenschutzangelegenheiten

Technische Maßnahmen	Organisatorische Maßnahmen
•	• Führen einer Übersicht über Verarbeitungstätigkeiten (Art. 30 DSGVO)
•	• Durchführung von Datenschutzfolgenabschätzungen, soweit erforderlich (Art. 35 DSGVO)
•	• Ext. Prüfung/Auditierung der Informationssicherheit (etwa im Rahmen von ISO-Zertifizierung)

Auftragskontrolle

Folgende Maßnahmen gewährleisten, dass personenbezogene Daten nur entsprechend der GEDISA-Weisungen verarbeitet werden und die durch die GEDISA beauftragten Unterauftragnehmer bei der Verarbeitung personenbezogener Daten mindestens das gleiche Schutzniveau wie die vorliegenden technischen und organisatorischen Maßnehmen bieten.

Technische Maßnahmen	Organisatorische Maßnahmen
•	• Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
•	• schriftliche Weisungen an den Auftragnehmer (z. B. durch Auftragsverarbeitungsvertrag)
•	• Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis/die Vertraulichkeit
•	• Auftragnehmer hat Datenschutzbeauftragten bestellt
•	• Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
•	• wirksame Kontrollrechte gegenüber der Auftragnehmerin vereinbart
•	• laufende Überprüfung der Auftragnehmerin und ihrer Tätigkeiten
•	• Prozess zur Erteilung und/oder Befolgung von Weisungen
•	• Unabhängige Auditierung der Weisungsgebundenheit
•	• Verpflichtung der Mitarbeiter auf das Datengeheimnis
•	• Vereinbarung von Konventionalstrafen für Verstöße gegen Weisungen
•	• dokumentiertes Verfahren zur Auswahl des Dienstleisters
•	• standardisiertes Vertragsmanagement zur Vor- und Nachkontrolle der Dienstleister

Vorfallsbehandlung

Folgende Maßnahmen gewährleisten, dass im Fall von Datenschutzverstößen Meldeprozesse ausgelöst werden.

Technische Maßnahmen	Organisatorische Maßnahmen
•	• Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Aufsichtsbehörden (Art. 33 DSGVO)
•	• Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Betroffenen (Art. 34 DSGVO)

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Folgende Maßnahmen gewährleisten, dass nur die personenbezogenen Daten verarbeitet werden, die tatsächlich verarbeitet werden müssen und dass Betroffene ausreichend und transparent über die Datenverarbeitung informiert werden.

Technische Maßnahmen	Organisatorische Maßnahmen
•	• Berücksichtigung bei der Kennzeichnung von Eingabefeldern in Onlineformularen als Pflichtfelder
•	• Sicherstellung der Verlinkung bzw. Kenntnisnahme der DS-Erklärung der Webseite vor Übermittlung von Daten
•	• Cookies – Einholung der Einverständniserklärung bei Einsatz von Trackingtools