Vereinbarung über die Nutzung eines „Intelligenten Sprachdialogsystems für Apotheken“

zwischen

gesund.de GmbH & Co. KG
Riesstraße 19
80992 München

(nachfolgend „**gesund.de**“)

und

Apotheke

(beide nachfolgend gemeinsam "**Parteien**")

Präambel

gesund.de unterstützt Leistungserbringer wie die Vor-Ort-Apotheken bei der Digitalisierung. Die Apotheke übernimmt die Arzneimittelversorgung, dabei ist sie Ansprechpartnerin und Beraterin hinsichtlich aller Fragen, die diese Versorgung betreffen. Hierzu zählen im Apothekenalltag auch administrative Aufgaben, wie die telefonische Auskunft gegenüber Patientinnen und Patienten zu Verfügbarkeiten von Produkten, zu Öffnungszeiten, Notdiensten und (Vor-)Bestellungsabwicklungen. Da diese telefonischen Auskünfte die Apotheke regelmäßig zeitlich stark einbinden, möchte die Apotheke Systeme einsetzen, um die Abwicklung von einfachen Kundenanfragen über das Telefon zu automatisieren.

Die Apotheke nutzt bereits durch gesund.de zur Verfügung gestellte Services. Hierzu haben die Parteien die "Vereinbarung über die entgeltliche Nutzung des gesund.de-Service" sowie die "gesund.de CardLink Vereinbarung" abgeschlossen.

Neben den vorstehend genannten Services stellt gesund.de der Apotheke unter Geltung dieser Nutzungsvereinbarung einen weiteren Service zur Verfügung. Dieser Service umfasst die Bereitstellung einer auf dem Einsatz von Künstlicher Intelligenz ("KI") basierenden Telefonlösung, die die Apotheke über den Apotheken-Telefonanschluss im Apothekenalltag nutzen kann.

1. Vertragsgegenstand

1.1. Diese Vereinbarung über die Nutzung eines „Intelligenten Sprachdialogsystems für Apotheken“ ("Vertrag") regelt die Nutzung der für die Apotheken durch gesund.de bereitgestellten Telefonlösung, die den Einsatz eines KI-basierten Telefonassistenten umfasst. Hierbei nutzt der Telefonassistent generative Künstliche Intelligenz, um automatisiert Kundenanrufe bei der Apotheke entgegenzunehmen und zu beantworten (nachfolgend "gesund.de **KI**RA" oder auch "gesund.de **KI**RA-Anwendung").

1.2. Die durch gesund.de bereitgestellte gesund.de **KI**RA-Anwendung umfasst die dafür notwendige technologische Infrastruktur, die der gesund.de **KI**RA-Anwendung zugrunde liegt, sowie die zur Nutzung notwendigen Einstellungen und Statistiken im Cockpit (Cockpit, wie in der Vereinbarung über die entgeltliche Nutzung des gesund.de-Service definiert).

1.3. Allgemeine Geschäftsbedingungen der Apotheke werden nicht Vertragsinhalt, auch wenn ihnen durch gesund.de nicht ausdrücklich widersprochen wird.

2. Nutzungsvoraussetzungen

2.1. Voraussetzung für die Nutzung der gesund.de **KI**RA-Anwendung für die Laufzeit dieses Vertrags ist:

a) Der Abschluss der Vereinbarung über die entgeltliche Nutzung des gesund.de-Service.

b) Der Abschluss der gesund.de CardLink Vereinbarung.

2.2. Die Apotheke gewährleistet für die Laufzeit dieses Vertrags die technische Integration der gesund.de **KI**RA-Anwendung in die Telefonanlage der Apotheke. Hierzu zählen insbesondere:

a) Die Weiterleitung von eingehenden Anrufen an eine von gesund.de zu benennende Telefonnummer aus dem deutschen Festnetz.

b) Die Zurverfügungstellung einer zweiten Telefonnummer zur Weiterleitung von Anrufen aus KIRA an die Apotheke.

2.3. Die Apotheke verpflichtet sich, die im Cockpit (Cockpit, wie in der Vereinbarung über die entgeltliche Nutzung des gesund.de- Service definiert) bereitgehaltenen Informationen und Schnittstellenverbindungen, aktuell zu halten. Sofern die Schnittstelle zur Warenwirtschaft der jeweiligen Apotheke nicht konfiguriert ist, nutzt KIRA bei Auskünften und Übermittlung von Bestellungen Standard-Apothekenverkaufspreise. Individuelle Verfügbarkeitsinformationen bezogen auf die jeweilige Apotheke können in diesem Fall nicht bereitgestellt werden.

3. Allgemeine Bestimmungen zur Beschaffenheit und Verfügbarkeit der gesund.de KIRA-Anwendung

3.1. gesund.de arbeitet für die Zurverfügungstellung und Implementierung der gesund.de **KI**RA-Anwendung mit externen Dritten zusammen. gesund.de übernimmt die Koordination und Kommunikation mit diesen.

3.2. Die Parteien werden die für sie geltenden rechtlichen Vorgaben einhalten und achten.

3.3. Bei Erfüllung der Einsatzvoraussetzungen gemäß Ziffer 2 sagt gesund.de eine Mindestverfügbarkeit der gesund.de **KI**RA-Anwendung in Höhe von mindestens 98,0% im Vertragsjahresmittel zu.

3.4. Die gesund.de **KI**RA-Anwendung gilt als nicht-verfügbar, wenn durch den Service Anrufe nicht angenommen und verarbeitet werden können.

3.5. Von der Zusage der Mindestverfügbarkeit ausgenommen sind Unterbrechungen der Verfügbarkeit wegen (i) Routinewartungsarbeiten innerhalb der dafür von gesund.de vorgesehener Zeitfenster; (ii) Maßnahmen zur Notfallwartung, insbesondere das Einspielen von Hot-Fixes und kritischen Sicherheitsupdates; sowie (iii) Umständen die von gesund.de nicht zu vertreten sind. Zu den von gesund.de nicht zu vertretenen Umständen zählen ins-besondere: (i) Fälle höherer Gewalt, (ii) Störungen oder Unterbrechungen der Funktionsfähigkeit oder Verfügbarkeit von IT-Systemen Dritter, die im Zusammenhang mit der Vertragssoftware eingesetzt werden, wobei die Verantwortung von gesund.de (vgl. Ziff. 3.1.) für eingesetzte Erfüllungsgehilfen unberührt bleibt; und (iii) Angriffe Dritter auf die zur Erbringung der Leistungen eingesetzten Infrastruktur.

3.6. gesund.de nimmt Routinewartungsarbeiten in der Regel außerhalb des regulären Apothekenbetriebs vor. Routinewartungsarbeiten mit Auswirkungen auf die Verfügbarkeit wird gesund.de in der Regel fünf (5) Werktage im Voraus anzeigen. Maßnahmen zur Notfallwartung außerhalb der Wartungsfenster für Routinewartungsarbeiten zeigt gesund.de der Apotheke möglichst zwölf (12) Stunden vorab an.

3.7. Die Apotheke wird gesund.de über nicht unerhebliche Unterbrechungen der vereinbarten Verfügbarkeit informieren.

4. Mitwirkungsverpflichtungen der Apotheke

4.1. Das Einhalten apothekenrechtlicher Vorgaben obliegt der Apotheke. An Vertragsschlüssen zwischen der Apotheke und ihren Kunden ist gesund.de nicht beteiligt. gesund.de prüft die vom Kunden an die Apotheke übermittelten Daten nicht, insbesondere nicht auf Richtigkeit, Vollständigkeit oder Plausibilität und macht sich diese Inhalte auch nicht zu eigen.

4.2. Sofern zur Einrichtung der gesund.de **KI**RA-Anwendung notwendig, wird die Apotheke technischem Personal Zugang zu und Zugriff auf die erforderlichen Systeme verschaffen und erforderliche Informationen beschaffen bzw. Auskünfte erteilen.

4.3. Die Apotheke ist zur Aufbewahrung von Informationen im Zusammenhang mit der Vorbestellung/dem Verkauf von Waren gesetzlich verpflichtet. Die Apotheke verwaltet die Aufbewahrung und Löschung dieser Vorgänge (einschließlich Vorbestellungen von RX-Produkten) in eigener Verantwortung nach den gesetzlichen Vorschriften.

4.4. Die Apotheke ist verpflichtet, ihre Zugangsdaten zur gesund.de **KI**RA-Anwendung geheim zu halten sowie eine unberechtigte Nutzung der Vertragssoftware durch Dritte zu verhindern. Erfährt die Apotheke vom Missbrauch der Zugangsdaten, so wird sie gesund.de unverzüglich darüber informieren. Die Apotheke haftet für einen von ihr zu vertretenden Missbrauch.

5. Gebühren

5.1. Der Apotheke entstehen – je nach ausgewähltem Paket – für die Nutzung der gesund.de **KI**RA-Anwendung während der Laufzeit der Vereinbarung die in **Anlage 1** aufgeführten Zahlungsverpflichtungen.

5.2. Sofern dem Kunden im Online-Bestellprozess (Vertragsabschluss) Sonderkonditionen (z.B. im Rahmen eines Messeangebots) angeboten wurden, gelten diese ergänzend zu den in Anlage 1 genannten Bedingungen.

5.3. Alle Gebühren verstehen sich zuzüglich der gesetzlichen Umsatzsteuer, sofern diese anfällt.

5.4. Die Apotheke erbringt alle Mitwirkungsleistungen inkl. der Einrichtung ihrer Telefonanlage auf eigene Kosten durch fachkundiges und für die jeweilige Mitwirkungsleistung hinreichend qualifiziertes Personal. Insb. trägt die Apotheke die ihr ggf. entstehenden Implementierungskosten für die Nutzung der gesund.de **KI**RA-Anwendung selbst.

6. Nutzungsbefugnisse und -beschränkungen

6.1. gesund.de gestattet der Apotheke für die Laufzeit dieses Vertrags die gesund.de **KI**RA-Anwendung zur Verwirklichung der in Ziffer 1 genannten Zwecke in ihrem Geschäftsbetrieb im Rahmen eines nicht ausschließlichen Nutzungsrechtes zu nutzen. Ein Weiterverkauf oder sonstige Gestattung der Nutzung der gesund.de **KI**RA-Anwendung durch Dritte ist nicht erlaubt.

6.2. Das Recht zur Nutzung umfasst auch das Recht zur Nutzung von Updates, Änderungen der gesund.de **KI**RA-Anwendung, die gesund.de im freien Ermessen zur Verfügung stellen kann.

6.3. Die Apotheke verpflichtet sich, die in der gesund.de **KI**RA-Anwendung enthaltenen Urheberschutzvermerke, wie Copyright-Vermerke und andere Rechtsvorbehalte, unverändert beizubehalten.

6.4. Die Übertragung der vorgenannten Nutzungsrechte an sonstige Dritte ohne Zustimmung der gesund.de ist untersagt; dies gilt auch für den Fall einer vollständigen oder teilweisen Veräußerung, Verpachtung oder Schließung des Geschäftsbetriebes der Apotheke.

6.5. Die Nutzung unterliegt ggf. weiterer, seitens der zur Bereitstellung und Implementierung der gesund.de **KI**RA-Anwendung genutzten externen Dritten geforderter Restriktionen (z.B. Acceptable Use Policy), welche von der Apotheke zu akzeptieren sind.

7. Gewährleistung

7.1. Bei Erfüllung der Einsatzbedingungen gemäß Ziffer 2 gewährleistet gesund.de den vertragsgemäßen Betrieb der gesund.de **KI**RA-Anwendung ohne Sachmängel und ohne Rechtsmängel. Die Gewährleistung erstreckt sich nicht auf Fehler, die durch Abweichen von den in Ziffer 2 vereinbarten Einsatzbedingungen verursacht werden.

7.2. Soweit der Apotheke der vertragsgemäße Gebrauch der Vertragssoftware durch einen Rechtsmangel ganz oder teilweise entzogen ist, kann gesund.de diesen Mangel nach eigener Wahl auch beseitigen, indem gesund.de

a) der Apotheke die erforderlichen Rechte zur vertragsgemäßen Verwendung der gesund.de **KI**RA-Anwendung verschafft; oder

b) die gesund.de **KI**RA-Anwendung so ändert, dass das Recht des Dritten der vertragsgemäßen Nutzung durch die Apotheke nicht mehr entgegensteht.

gesund.de wird berechtigte Interessen der Apotheke dabei angemessen berücksichtigen.

7.3. gesund.de gewährleistet nicht die inhaltliche Richtigkeit oder Vollständigkeit der durch den KI-basierten Telefonassistenten erneuten Antworten und sonstigen Inhalte. Dem Kunden ist bewusst, dass beim Einsatz von KI inhaltliche Fehler (z.B. durch sog. Halluzinationen) sich derzeit technisch nicht ausschließen lassen. Ferner gewährleistet gesund.de nicht, dass die Kunden der Apotheke den KI-basierten Telefonassistenten als Kommunikationskanal akzeptieren. Es obliegt der Apotheke ihren Kunden ggf. alternative Kommunikationskanäle anzubieten.

7.4. Im Übrigen gelten bei Mängeln die §§ 535 ff. BGB mit der Maßgabe, dass die verschuldensunabhängige Haftung für bei Vertragsschluss vorhandene Mängel gemäß § 536a Abs. 1, 1. Alt. BGB ausgeschlossen ist.

8. Support und Updates

8.1. gesund.de steht für die Dauer der Laufzeit dieses Vertrags der Apotheke während der gesund.de-Geschäftszeiten unter kira-support@gesund.de als Ansprechpartner zur Verfügung.

8.2. gesund.de ist berechtigt, Daten, die im Rahmen der Erbringung der vertraglich geschuldeten Leistungen erhoben wurden, während und auch nach Beendigung dieses Vertrages zu anonymisieren oder aggregieren und in dieser Form zur internen Analyse, Weiterentwicklung der gesund.de Services und statistischen Auswertung zu verwenden. Daten im vorstehenden Sinne sind sämtliche im Rahmen der Erbringung der vertraglich geschuldeten Leistungen erhobenen personenbezogenen, pseudonymisierten oder anonymisierten Informationen sowie damit verbundene Metadaten.

9. Laufzeit dieses Vertrags

9.1. Der Vertrag tritt am Tag des Vertragsschlusses in Kraft („Vertragsbeginn“). Ab Vertragsbeginn läuft der Vertrag für eine Mindestlaufzeit von zwölf (12) Monaten („Erstlaufzeit“). Die monatliche Gebühr wird erstmalig ab dem auf das Onboarding folgenden vollen Monat in Rechnung gestellt.

9.2. Wird der Vertrag nicht von einer Partei mit einer Frist von drei (3) Monaten zum Ende der Erstlaufzeit in Textform (z.B. E-Mail) gekündigt, verlängert er sich jeweils automatisch um weitere zwölf (12) Monate („Verlängerungsperiode“). Gleiches gilt jeweils für das Ende jeder Verlängerungsperiode. Die Beendigung des Vertrags erfolgt immer zum Ende des letzten Vertragsmonats.

9.3. Sofern dem Kunden im Online-Bestellprozess ein Sonderkündigungsrecht (z.B. eine Testphase) angeboten wurde, gilt dieses Sonderkündigungsrecht ergänzend.

9.4. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt. Anstelle einer Kündigung aus wichtigem Grund, kann gesund.de den Zugang der Apotheke zur gesund.de **KI**RA-Anwendung sperren.

9.5. Kündigungen bedürfen der Textform und sind an die E-Mail-Adresse **KIRA@gesund.de** zu richten. Für die Fristwahrung ist der rechtzeitige Zugang maßgeblich.

9.6. Nach Vertragsbeendigung wird gesund.de den Zugang der Apotheke zur gesund.de **KI**RA-Anwendung sperren. Ferner enden alle gegenüber der Apotheke eingeräumten Rechte an der Vertragssoftware und Updates.

10. Haftung

10.1. gesund.de haftet unbeschränkt bei Vorsatz, grober Fahrlässigkeit sowie bei schuldhafter Verletzung von Leben, Körper oder Gesundheit.

10.2. Bei leichter Fahrlässigkeit haftet gesund.de darüber hinaus nur bei Verletzung wesentlicher Vertragspflichten, also Pflichten, deren Erfüllung die ordnungsgemäße Durchführung des Vertrages überhaupt erst ermöglicht oder deren Verletzung die Erreichung des Vertragszwecks gefährdet und auf deren Einhaltung der Vertragspartner regelmäßig vertrauen darf. Die Haftung der gesund.de ist in diesen Fällen auf den bei Vertragsschluss vorhersehbaren, vertragstypischen Schaden begrenzt. Die unbeschränkte Haftung nach Ziffer 10.1. bleibt hiervon unberührt. Über Ziffer 10.1 und Ziffer 10.2 hinaus haftet gesund.de nicht für leichte Fahrlässigkeit.

10.3. Die vorstehenden Haftungsbeschränkungen gelten auch zugunsten von Mitarbeitern, Vertretern, Organen und Erfüllungsgehilfen von gesund.de.

10.4. Sämtliche vorstehenden Haftungsbeschränkungen gelten nicht für die Haftung bei Fehlen garantierter Eigenschaften, bei Arglist, sowie für Ansprüche nach dem Produkthaftungsgesetz.

11. Datenschutz

11.1. Soweit die Parteien im Rahmen der Vertragsdurchführung personenbezogene Daten verarbeiten, werden sie die darauf jeweils anwendbaren Gesetze und sonstigen Regularien, insbesondere die anwendbaren Bestimmungen des Datenschutzrechts, einhalten.

11.2. Die Parteien stimmen überein, dass die Apotheke unter dieser Vereinbarung die datenverarbeitende Stelle ist und schließen diesbezüglich eine Vereinbarung zur Auftragsverarbeitung („AVV“) **Anlage 2**. In seinem Anwendungsbereich hat der AVV Vorrang gegenüber den Regelungen dieses Vertrags. Die Apotheke trägt die alleinige Verantwortung für die Zulässigkeit der Verarbeitung der personenbezogenen Daten im Auftragsverhältnis und für die Erfüllung der maßgeblichen Anforderungen des anwendbaren Datenschutzrechts, insbesondere die ordnungsgemäße Information Betroffener (Art. 12 ff. DSGVO).

12. Vertraulichkeit

12.1. „Vertrauliche Informationen“ einer Partei sind Informationen zu wettbewerbsrelevantem Know-how, als vertraulich gekennzeichnete oder sonst auf Grundlage eines objektiven Empfängerhorizonts als vertraulich erkennbare Informationen sowie sonstige Geschäftsgeheimnisse.

12.2. Die Parteien werden ihnen im Zuge der Vertragsanbahnung und -durchführung bekanntwerdende Vertrauliche Informationen der jeweils anderen Partei

a) vertraulich behandeln und ausschließlich zur Vertragsdurchführung verwenden;
a) Arbeitnehmern und Dritten nicht offenlegen oder zugänglich machen, außer soweit dies für die Vertragsdurchführung erforderlich ist (need-to-know); und
b) durch angemessene und geeignete Maßnahmen gegen den Zugriff durch unberechtigte Personen schützen (z. B. Zugangskontrolle, Verschlüsselung).

12.3. Ziffer 12.1 gilt nicht für Vertrauliche Informationen, die

a) eine Partei von Dritten rechtmäßig, insbesondere ohne Verstoß gegen eine Vertraulichkeitsverpflichtung erhalten hat oder erhält;
b) bei Vertragsschluss bereits allgemein bekannt waren oder nachträglich ohne Verstoß gegen die in diesem Vertrag enthaltenen Verpflichtungen allgemeinbekannt werden;
c) bei einer Partei bereits vor Aufnahme der Geschäftsbeziehungen vorhanden waren und keiner Verschwiegenheitsverpflichtung unterliegen; oder
d) durch eine Partei unabhängig entwickelt werden.

12.4. Die Parteien sind zur Verwendung und Offenlegung Vertraulicher Informationen berechtigt, soweit sie hierzu gesetzlich oder behördlich verpflichtet sind. In einem solchen Fall wird die betreffende Partei die andere Partei in Text- oder Schriftform informieren.

12.5. Die Vertraulichkeitspflichten gelten für drei (3) Jahre über die Beendigung der Vertragsbeziehung zwischen den Parteien hinaus.

13. Öffentlichkeitsarbeit

13.1. Die Entscheidung über eine Veröffentlichung bzw. Berichterstattung über die Vermarktung der gesund.de **KI**RA-Anwendung ("Öffentlichkeitsarbeit") obliegt gesund.de. Sofern gesund.de mit der Öffentlichkeitsarbeit begonnen hat und der Apotheke Marketing-Materialien bereitstellt, ist die Apotheke berechtigt selbst mit dem Einsatz der gesund.de **KI**RA-Anwendung zu werben. Für sämtliche Marketingaktionen der Apotheke sind ausschließlich die von gesund.de bereitgestellten Materialien zu verwenden.

13.2. Sofern sich gesund.de zugunsten der Öffentlichkeitsarbeit entscheidet, erfolgen Veröffentlichungen mit konkretem Bezug zur teilnehmenden Apotheke nur nach vorheriger Zustimmung derselben.

13.3. Stimmt die Apotheke der Veröffentlichung unter konkreter Bezugnahme auf die eigene Apotheke zu, so stellt sie auf Anforderung der gesund.de unentgeltlich geeignetes

Bildmaterial und wörtliche Zitate zur Verfügung, die gesund.de für die Öffentlichkeitsarbeit und für die Bewerbung der gesund.de **KI**RA-Anwendung verwenden darf und räumt hierzu gesund.de bereits hiermit alle erforderlichen Rechte in Form einer einfachen, zeitlich, räumlich und inhaltlich uneingeschränkten weiterübertragbaren Lizenz ein.

14. Änderung dieses Vertrags

14.1. gesund.de kann die Vereinbarung ändern, wenn und soweit dies aus triftigem, bei Vertragsschluss nicht vorhersehbaren Grund, erforderlich ist und das Verhältnis von Leistung und Gegenleistung nicht zu Ungunsten der Apotheke verschoben wird, so dass die Änderung für die Apotheke zumutbar ist. Ein triftiger Grund liegt vor, wenn die Anpassung notwendig ist, um die Leistungen an den Stand der Technik und Sicherheit, die Entwicklung rechtlicher und aufsichtsbehördlicher Anforderungen insbesondere in Bereichen Apothekenregulierung und Medizin, Produktsicherheit, Datenschutz, Telekommunikation und Verbraucherschutz sowie Marktentwicklungen insbesondere Kundenerwartungen an vergleichbare Leistungen beispielsweise im Hinblick auf Performance, Speicherkapazitäten, Nutzerfreundlichkeit und Effizienz anzupassen.

14.2. Über Änderungen dieses Vertrags wird gesund.de die Apotheke unter Mitteilung der geänderten Bedingungen mindestens dreißig (30) Tage vorab informieren. Die Änderung ist in Textform zur Verfügung zu stellen. Die elektronische Form wird ausdrücklich zugelassen.

14.3. Die Änderungen werden Vertragsbestandteil, wenn die Apotheke nicht binnen dreißig (30) Tagen nach Zugang der in Textform oder elektronischer Form abgefassten Änderungsmitteilung in Textform widerspricht. Fällt das Fristende auf einen Sonn- oder Feiertag gilt als Fristablauf das Ende des nächsten Werktages. Widerspricht die Apotheke rechtzeitig in Textform, wird die Vereinbarung zu den bisherigen Bedingungen fortgesetzt. gesund.de wird in der Änderungsmitteilung auf das Widerspruchsrecht der Apotheke und diese Folgen hinweisen.

15. Preisanpassungen

15.1. Zur Beseitigung nachträglich entstehender Äquivalenzstörungen, insbesondere zur Anpassung an gestiegene oder gesunkene Kosten für Bereitstellung und Betrieb der Vertragssoftware (z.B. Lohnkosten, Stromkosten, Infrastrukturkosten), kann gesund.de die Gebühren (Anlage 1) für die Vertragssoftware in jedem Vertragsjahr einmalig angemessen anpassen. Eine Erhöhung der Nutzungsgebühr darf die für den Erzeugerpreisindex für IT-Dienstleistungen (DL-IT) des Statistischen Bundesamts ausgewiesene Veränderungsrate zum Vorjahr (Jahresdurchschnitt), zuzüglich eineinhalb (1,5) Prozentpunkte dabei nicht übersteigen.

15.2. gesund.de wird den Kunden rechtzeitig über die Anpassung der Nutzungsgebühr informieren. Ziff. 14.2 und 14.3 finden entsprechende Anwendung

16. Anwendbares Recht und Gerichtsstand

16.1. Für die Vereinbarung sowie alle Ansprüche, Rechte und Pflichten aus oder im Zusammenhangmit der Vereinbarung gilt das Recht der Bundesrepublik Deutschland. Das UN-Kaufrecht (CISG) sowie das internationale Privatrecht sind ausgeschlossen.

16.2. Ausschließlicher Gerichtsstand für sämtliche Streitigkeiten der Parteien aus oder im Zusammenhang mit der Vereinbarung ist, sofern die Apotheke Kaufmann ist, München, Deutschland.

17. Schlussbestimmungen

17.1. Die Apotheke kann nur mit unstreitigen oder rechtskräftig festgestellten Ansprüchen aus diesem Vertrag gegenüber gesund.de aufrechnen und nur aufgrund solcher Ansprüche von einem Zurückbehaltungsrecht Gebrauch machen.

17.2. Die Präambel sowie die im Vertragstext genannten Anlagen sind wesentlicher Bestandteil dieses Vertrags. Nebenabreden bestehen nicht.

17.3. Sind oder werden einzelne Bestimmungen dieses Vertrags unwirksam, so bleibt dessen Gültigkeit im Übrigen unberührt. Ungültige Bestimmungen sind einvernehmlich durch solche zu ersetzen, die unter Berücksichtigung der Interessenlage beider Parteien den gewünschten wirtschaftlichen Zweck zu erreichen geeignet sind. Entsprechendes gilt für die Ausfüllung von Lücken, die sich in diesem Vertrag herausstellen könnten.

17.4. Dieser Vertrag kann wirksam auch online (z. B. über ein Web- oder App-basiertes Registrierungs- oder Bestätigungssystem) oder telefonisch geschlossen werden, sofern die wesentlichen Vertragsinhalte in Textform im Sinne des § 126b BGB (z. B. E-Mail) bestätigt werden. Soweit in diesem Vertrag keine strengere Form vorgeschrieben ist, bedürfen Änderungen, Ergänzungen sowie sonstige auf seiner Grundlage abzugebende Erklärungen der Textform im Sinne des § 126b BGB (z. B. E-Mail).

Anlage 1 - Paketpreise

1. gesund.de bietet den Apotheken folgende drei Paketgrößen mit Inklusivminuten an:

Paket	Monatliche Inklusivminuten	Monatliche Gebühr (in Euro)	Einmalige Gebühr (in Euro)	Gebühr nach Ausschöpfung der Inklusiv-minuten (in Euro)
Basis	375	79	599	0,23/Minute
Komfort	800	159	599	0,22/Minute
Profi	1600	299	599	0,20/Minute

2. Die Apotheke wählt das ihren Bedürfnissen entsprechende Paket im Online-Bestellprozess aus. Eine nachträgliche Änderung ist jeweils mit einem Vorlauf von 10 Werktagen zum nächsterreichbaren Monat per E-Mail an KIRA@gesund.de möglich.
3. Die verbrauchten Minuten werden in einem minutengenauen Abrechnungstakt erfasst.
4. Die monatliche Gebühr wird erstmalig ab dem auf das Onboarding folgenden Monat in Rechnung gestellt.
5. Etwaige Anbindungs- und Verbindungskosten, die der jeweilige Telekommunikations-anbieter der Apotheke in Rechnung stellt, sind von der Apotheke zu tragen.
6. Telefonate die über die im gesund.de Cockpit hinterlegten Backup-Nummer erfolgen, werden mit 0,02€/Minute abgerechnet.
7. Ab der 3. bis 4. teilnehmenden Filiale der Apotheke wird nachfolgender Filialnachlass auf die monatliche Gebühr der 3. bzw. 4. teilnehmenden Filiale gewährt:

   Basis-Paket: 10 Euro Rabatt/Monat
   Komfort-Paket: 20 Euro Rabatt/Monat
   Profi-Paket: 20 Euro Rabatt/Monat

Anlage 2 - Vertrag über die Auftragsverarbeitung

Zwischen

gesund.de GmbH & Co. KG
Riesstraße 19
80992 München

– im Folgenden "**Auftragnehmer**" genannt –

und
Apotheke

– im Folgenden "**Auftraggeber**" genannt –

– einzeln als "**Partei**" bezeichnet, zusammen als "die **Parteien**" bezeichnet –

Präambel

Der Auftragnehmer erbringt für Vor-Ort-Apotheken in Deutschland Dienstleistungen im Bereich intelligenter Sprachdialogsysteme, mit dem Ziel, telefonische Prozesse durch moderne Technologien teil- oder vollautomatisiert zu unterstützen. Die telefonischen Anfragen erfolgen dabei weiterhin über die jeweilige Telefonnummer der teilnehmenden Apotheke und werden dabei auf das System des Auftragnehmers weitergeleitet. Die Erbringung dieser Leistungen erfolgt auf Grundlage eines gesondert geschlossenen Hauptvertrags zwischen den Parteien.

Hierfür schließen die Parteien diesen Vertrag über die Auftragsverarbeitung ("AVV") gemäß Art. 28 Datenschutz-Grundverordnung ("DSGVO"). Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen sind in Annex 1 näher beschrieben. Dieser AVV findet nur Anwendung auf die Verarbeitung personenbezogener Daten ("pbD") im Zusammenhang mit der beschriebenen Dienstleistung.

1. Gegenstand, Dauer und Spezifizierung des 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 Strafgesetzbuch.

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").

2.3 Erteilt der Auftraggeber dem Auftragnehmer Weisungen, welche über die vertraglich vereinbarten Leistungen hinausgehen, so kann der Auftragnehmer dem Auftraggeber die daraus resultierenden Kosten in Rechnung stellen.

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 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 organisatorischen Maßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht 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 Art. 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 Die Parteien benennen einander jeweils einen Ansprechpartner für alle im Zusammenhang mit diesem AVV anfallenden Datenschutzfragen (vgl. Annex 2).

3.8 Der Auftragnehmer berichtigt 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.

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 Art. 82 DSGVO verpflichten sich Auftraggeber und Auftragnehmer, sich hinsichtlich der Verifizierung der Aktivlegitimation und bei der Abwehr des jeweiligen Anspruches gegenseitig zu unterstützen.

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 Art. 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 Art. 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 und stellt sicher, dass der Unterauftragsverarbeiter die personenbezogenen Daten nicht zu eigenen Zwecken verarbeitet.

7.2 Unter-Auftragsverarbeiter 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. 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. 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.

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

7.4 Beauftragt der Auftragnehmer einen Unter-Auftragsverarbeiter, so hat er mit diesem einen Vertrag zu schließen, der den datenschutzrechtlichen Anforderungen dieses AVV inhaltlich entspricht und dem Unter-Auftragsverarbeiter mindestens gleichwertige Verpflichtungen auferlegt. 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, 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. Laufzeit

Der AVV gilt für den Zeitraum der Geltung des Hauptvertrages. Eine Beendigung des AVV führt automatisch zur Beendigung der Berechtigung zur Nutzung der intelligenten Sprachdialogsysteme.

9. Haftung

Es gelten die Regelungen aus Art. 82 DSGVO.

10. Informationspflichten, Schriftformklausel, Rechtswahl

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 über und das Eigentum an den Daten ausschließlich beim Auftraggeber als "Verantwortlicher" im Sinne der DSGVO liegen.

10.1 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: Technische und organisatorische Maßnahmen (TOM)

10.2 Für Änderungen und Ergänzungen dieses AVV gelten die Formvorschriften des Hauptvertrages.

10.3 Bei Widersprüchen geht dieser AVV in seinem Anwendungsbereich den Regelungen des Hauptvertrages vor.

10.4 Sollten einzelne Teile dieses AVV unwirksam sein, so berührt dies die Wirksamkeit des AVV im Übrigen nicht.

10.5 Auf diesen AVV findet das für den Hauptvertrag geltende Recht Anwendung. Ausschließlicher Gerichtsstand ist der für die Nutzungsbedingungen vereinbarte Gerichtsstand.

Annex 1: Angaben zur Verarbeitung

1.1 Art und Zweck der Verarbeitung sind im Hauptvertrag konkretisiert und umfassen insbesondere:

Der Gegenstand der Auftragsverarbeitung ist im Hauptvertrag ausführlich beschrieben. Im Wesentlichen ist hiervon Folgendes umfasst: Die Erbringung von Dienstleistungen im Bereich KI-gestützter Sprachdialogsysteme zur Unterstützung und (teil-)automatisierten Bearbeitung telefonischer Anfragen an den Auftraggeber.

Art und Zweck der Verarbeitung sind im Hauptvertrag konkretisiert und umfassen insbesondere:

- die Annahme, Verarbeitung und strukturierte Weiterleitung telefonischer Anfragen, die über die zentrale Rufnummer der Apotheke eingehen,
- die (teil-)automatisierte Beantwortung typischer und wiederkehrender Fragen (z. B. zu Öffnungszeiten, Notdiensten, Parkmöglichkeiten, digitalen Services, Barrierefreiheit),
- die Unterstützung bei Bestell- und Reservierungsvorgängen, einschließlich Informationen zur Verfügbarkeit, dem Status von E-Rezepten und der Organisation des Botendienstes,
- die Bereitstellung apothekenbezogener Informationen (z. B. zu Impfangeboten oder digitalen Services),
- die Übergabe relevanter Gesprächsinhalte an das Apothekenteam zur weiteren Bearbeitung,
- die Verarbeitung und Analyse von Spracheingaben (z. B. zur Spracherkennung, Transkription oder Dialogoptimierung),
- die vorübergehende Speicherung oder Aufzeichnung von Sprachdaten, soweit dies zur technischen Erbringung oder Qualitätssicherung erforderlich und vertraglich vorgesehen ist,
- die technische Verarbeitung zur Sicherstellung, Weiterentwicklung und Qualitätssicherung der Sprachverarbeitungssysteme,
- sowie die Verarbeitung von Gesprächsdaten (einschließlich Transkripten) zur Optimierung der zugrunde liegenden Sprachmodelle und KI-Komponenten, ausschließlich im Rahmen der vertraglich vereinbarten Leistung und auf Weisung des Auftraggebers.

Zur Weiterentwicklung und Qualitätssicherung kann der Auftragnehmer einen Unterauftragsverarbeiter einsetzen, der Gesprächsdaten einschließlich Transkripten verarbeitet. Eine solche Verarbeitung erfolgt ausschließlich auf Grundlage einer datenschutzkonformen Vereinbarung gemäß Art. 28 Abs. 4 DSGVO, im Rahmen des erteilten Auftrags und auf ausdrückliche Weisung des Auftraggebers. Die Daten werden in diesem Fall nicht pseudonymisiert verarbeitet. Der Auftragnehmer stellt sicher, dass der eingesetzte Unterauftragsverarbeiter geeignete technische und organisatorische Maßnahmen zum Schutz der Daten trifft und die Verarbeitung ausschließlich im Auftrag und nicht zu eigenen Zwecken erfolgt.

1.2 Die Verarbeitung betrifft die nachfolgend genannten Arten von Daten:

Im Rahmen der beschriebenen Zwecke werden insbesondere folgende Arten personenbezogener Daten verarbeitet:

- Stammdaten (z. B. Name, ggf. Geburtsdatum oder Alter)
- Kontaktdaten (z. B. Telefonnummer, ggf. Adresse bei Botendienstanfragen)

- Gesundheitsbezogene Angaben, sofern vom Anrufenden freiwillig mitgeteilt (z. B. Informationen zu Rezepten, Medikamenten, Impfbedarf)
- Kommunikationsinhalte (z. B. Fragen zu Produkten, Services, Öffnungszeiten, Anfahrt etc.)
- Bestell- oder Lieferinformationen (z. B. Statusabfragen, Reservierungen, Botendienstaufträge)
- Pseudonymisierte Gesprächstranskripte
- Metadaten des Anrufs (z. B. Datum, Uhrzeit, Dauer, technische Verbindungsdaten)

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

Von der Verarbeitung betroffen sind insbesondere:

- Anrufende Personen, die telefonisch Kontakt mit der Apotheke aufnehmen, insbesondere Kundinnen und Kunden, Patientinnen und Patienten sowie sonstige Personen, die Informationen oder Leistungen der Apotheke erfragen oder in Anspruch nehmen möchten.

Annex 2: Liste und Kontaktdaten der Ansprechpartner

1. Auftraggeber

Ansprechpartner für Weisungen und Datenschutz:

Name	Telefon	E-Mail

Der Datenschutzbeauftragte beim Auftragnehmer ist:

Kontaktinformationen	E-Mail

2. Auftragnehmer

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
Vanessa Martin	VMartin@intersoft-consulting.de

Im Falle eines Wechsels oder einer längerfristigen Verhinderung verpflichtet sich jede Partei, die Kontaktdaten einer geeigneten Vertretung oder Nachfolgeperson unverzüglich mitzuteilen.

Annex 3: Technische und organisatorische Maßnahmen (TOM) nach Art. 32 DSGVO

Schutzklasse: Hoch

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. Eine Pseudonymisierung von Daten ist vom Auftragsverarbeiter zu fordern, wenn die Durchführung der übertragenen Datenverarbeitungsaufgaben durch die Pseudonymisierung nicht beeinträchtigt wird. Ggf. sind hier Unterscheidungen zwischen Produktiv-, Test- und Schulungsdaten/ - Systemen vorzunehmen und differenzierte Maßnahmen festzulegen.

b. Verschlüsselung

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

- Externe Webschnittstellen sind nach Stand der Technik verschlüsselt (HTTPS).
- Besonders schützenswerte Daten werden nach Stand der Technik verschlüsselt in der Datenbank abgelegt.

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

a. Gewährleistung der Belastbarkeit der Systeme auf Dauer

Hierzu gehören geeignete Maßnahmen, die schon in der Phase vor Durchführung der Datenverarbeitung durch den Auftragsverarbeiter zu ergreifen sind. Darüber hinaus ist auch eine kontinuierliche Überwachung der Systeme erforderlich.

- Regelmäßige Schulung des eingesetzten Personals (Management und sonstige interne und externe Mitarbeiter entsprechend dem Gebot zur Sicherstellung der Integrität und Vertraulichkeit der Datenverarbeitung zu handeln (mindestens einmal im Jahr).
- Dynamische Prozesse und Speicherzuschaltung.
- Load-Balancing.
- Belastungsgrenze für das jeweilige Datenverarbeitungssystem im Voraus über das notwendige Minimum ansetzen.

b. Zugriffskontrolle

Ziel der Zugriffskontrolle ist es, zu gewährleisten, dass nur die zur Benutzung eines Datenverarbeitungssystems Berechtigtenausschließlich auf die ihrer aufgabenbezogenen Zugriffsberechtigung unterliegenden pers. Daten zugreifen können, und dass pers. Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Die Umsetzung der folgenden Maßnahmen unterstützt diese Forderung.

- Alle Mitarbeiter, die mit personenbezogenen Daten Umgang haben, sind gesondert (z.B. durch Vertrag, Verpflichtungserklärung) oder gesetzlich zur Verschwiegenheit verpflichtet.
- Implementieren eines ausreichend differenzierten Rollen- und Berechtigungsmodells
- Verwendung von Benutzerkennungen.
- Identifikation und Authentifizierung der Benutzer.
- Zeitliche Begrenzung der Zugriffsmöglichkeiten.
- Zeitliche Begrenzung der Datenverarbeitung (z. B. durch Löschung von pers. Daten, die nicht mehr erforderlich sind).
- Kontrolle der Aktivitäten der Systemadministration.
- Einsatz von Verschlüsselungsverfahren.
- Trennung von Test und Produktionsbetrieb.
- Abschottung interner Netze.
- Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger.

c. Eingabekontrolle

Die Eingabekontrolle soll gewährleisten, dass nachvollzogen werden kann, wer, wann, welche pers. Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt hat.

Personenbezogene Daten können per Webinterface ausschließlich vom eingeloggten Benutzer selbst verändert werden. Eine derartige Änderung ist lediglich für zwei Wochen über die Logfiles nachvollziehbar.

Eine Veränderung durch einen Datenbankadministrator direkt in der Datenbank ist möglich, aber nicht vorgesehen.

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

Die Verfügbarkeitskontrolle soll sicherstellen, dass pers. Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Die Umsetzung der folgenden Maßnahmen unterstützt diese Forderung.

- Regelmäßige Datensicherung.
- Kontrolle der Datensicherung durch testweises Zurückspielen von Daten
- Durchführung einer Risiko- und Schwachstellenanalyse für den gesamten Datenverarbeitungsbereich.
- Formalisierte Freigabeverfahren für neue Datenverarbeitungsverfahren und bei wesentlichen Änderungen in bestehenden Verfahren.
- Einsatz geprüfter Fremdsoftware.
- Einsatz der Fernwartung.
- Erlass von Sicherheitsrichtlinien.

4. Regelmäßige Überprüfungen von Subauftragnehmern (Auftragskontrolle)

Ziel der Auftragskontrolle ist es, zu gewährleisten, dass pers. Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Zu diesem Zweck stellt der Auftragnehmer auch sicher, dass der Auftraggeber das Recht hat, auch bei Unterauftragnehmer die hier vereinbarten Überprüfungen vorzunehmen.

Die Umsetzung der folgenden Maßnahmen unterstützt diese Forderung.

- Schriftlicher Vertrag.
- Klare Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer.
- Definition von Sicherheitsmaßnahmen.

Regelmäßige Kontrolle der ordnungsgemäßen Vertragsausführung.