

Auftragsverarbeitungsvertrag

nach Art. 28 Abs. 3 DSGVO

zwischen

der teilnehmenden Apotheke

- nachfolgend "**Auftraggeber**" genannt –

und

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

- nachfolgend "**Anbieter**" genannt,

zusammen auch die "**Parteien**" oder einzeln als die "**Partei**"

1. Präambel

- 1.1 Der Anbieter erbringt für den Auftraggeber Dienste im Bereich des vom Anbieter betriebenen "gesund.de"-Service. Der gesund.de-Service umfasst die Leistungen verschiedener Dienste, deren Gegenstand die Kommunikation zwischen Auftraggeber und ihren Kunden via App und Web ist. Ein Teil dieser Dienste ist das vom Anbieter zur Verfügung gestellte Online-Terminbuchungstool. Hierfür haben der Anbieter und der Auftraggeber einen Hauptvertrag abgeschlossen ("**Hauptvertrag**"). Im Rahmen der Zurverfügungstellung dieses Tools für den Auftraggeber werden personenbezogene Daten von betroffenen Personen erhoben, verarbeitet und auf diese zugegriffen. Aus datenschutzrechtlicher Sicht ist der Auftraggeber der Verantwortliche und der Anbieter der Auftragsverarbeiter.
- 1.2 Dieser Auftragsverarbeitungsvertrag ("**Vertrag**") legt die Datenschutzverpflichtungen der Parteien im Rahmen der Erbringung der Dienstleistungen fest. Er gilt für alle vom Anbieter zu erbringenden Dienstleistungen, bei denen der Anbieter, seine Mitarbeiter oder ein im Namen vom Anbieter handelnder Dritter als Auftragsverarbeiter mit personenbezogenen Daten in Kontakt kommt und basiert auf den Bestimmungen von Art. 28 Datenschutz-Grundverordnung und den in der Datenschutz-Grundverordnung enthaltenen Definitionen.
- 1.3 Im Fall eines Widerspruchs zwischen diesem Vertrag und dem Hauptvertrag sowie dessen Anhängen oder einer anderen Vereinbarung zwischen den Parteien, haben die Bestimmungen dieses Vertrages Vorrang.

2. Definitionen

- 2.1 Alle hier verwendeten Begriffe in Großbuchstaben, die hier nicht anderweitig definiert sind, haben die Bedeutung, die dem jeweiligen Begriff in der DSGVO und dem Bundesdatenschutzgesetz zugewiesen wird.
- 2.2 "**Geltende Datenschutzgesetze**" bezeichnet alle anwendbaren weltweiten Rechtsvorschriften zum Datenschutz und zum Schutz der Privatsphäre, die für die jeweilige Partei in ihrer Rolle als verarbeitende Stelle personenbezogener Daten im Rahmen des Vertrags gelten, einschließlich, aber nicht beschränkt auf die Verordnung (EU) 2016/679 (die "Allgemeine

Datenschutzverordnung" oder "**DSGVO**") und dem Bundesdatenschutzgesetz ("**BDSG**"), jeweils in der jeweils geänderten, aufgehobenen, konsolidierten oder ersetzten Fassung.

3. Beschreibung der Verarbeitung

3.1 Der Anbieter ermöglicht im Rahmen des Online-Terminbuchungstools die Buchung von Terminen für den Nutzer der App bzw. der Webseite von gesund.de bei der teilnehmenden Apotheke, aber auch für Laufkundschaft der Apo. Diese Termine dienen der Erbringung von bestimmten Gesundheitsleistungen für den Nutzer. Dabei werden personenbezogene Daten der Nutzer inklusive Gesundheitsdaten Gegenstand der folgenden Verarbeitungen sein:

- Erhebung, Speicherung und Verarbeitung der personenbezogenen Daten beim Anbieter und Zurverfügungstellung an den Auftraggeber für die verschiedenen Funktionen, wie z.B. Anzeige verfügbarer Gesundheitsleistungen, Terminbuchung und -bestätigung, Erinnerungen, etc.

3.2 Dabei werden die folgenden personenbezogene Daten der Nutzer verarbeitet:

- Anrede,
- Name
- pseudonyme Kundenkennung,
- Stamapotheke
- Mobiltelefonnummer
- Stornierungsangaben
- Kommunikationsdaten
- Protokolldaten
- E-Mail-Adresse,
- ausgewählte Apotheke,
- ausgewählte Gesundheitsleistung und damit einhergehend ggf. Gesundheitsdaten des Nutzers,
- Datum, Uhrzeit und Status des Termins,
- Angaben zum Versicherungsstatus sowie
- weitere im Rahmen der Terminbuchung abgefragte Angaben.

3.3 Der Anbieter verarbeitet die personenbezogenen Daten ausschließlich im Auftrag und nach Weisung des Auftraggebers, sofern der Anbieter nicht durch die anwendbaren Gesetze zu einer anderen Verarbeitung verpflichtet ist. Die Parteien sind sich darüber einig, dass der Hauptvertrag (einschließlich dessen Anhänge) und dieser Vertrag zusammen mit ihrer Nutzung der Dienstleistungen die vollständigen und endgültigen Anweisungen des Auftraggebers den Anbieter in Bezug auf die Verarbeitung personenbezogener Daten darstellen, und dass alle zusätzlichen Anweisungen, die über den Umfang der Anweisungen hinausgehen, eine vorherige schriftliche Vereinbarung zwischen den Parteien erfordern.

3.4 Ist der Anbieter der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat der Anbieter den Auftraggeber unverzüglich darauf hinzuweisen. Der Anbieter ist berechtigt, die Durchführung der betreffenden Weisung so lange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Anbieter darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

3.5 Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nichts anderes ergibt.

4. Pflichten des Auftraggebers

4.1 Im Rahmen des Vertrags und bei der Nutzung der Dienste ist der Auftraggeber für die Einhaltung aller Anforderungen verantwortlich, die für ihn gemäß den geltenden Datenschutzgesetzen in Bezug auf die Verarbeitung personenbezogener Daten und die den Anbieter erteilten Anweisungen gelten. Dies gilt insbesondere für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO.

4.2

5. Pflichten des Auftragsverarbeiters

5.1 Der Anbieter stellt sicher, dass die zur Verarbeitung personenbezogener Daten befugten Personen sich zur Vertraulichkeit bezüglich personenbezogener Daten verpflichtet haben oder einer entsprechenden gesetzlichen Geheimhaltungspflicht unterliegen.

5.2 Der Anbieter benachrichtigt den Auftraggeber unverzüglich, nachdem er von einer Verletzung des Schutzes personenbezogener Daten Kenntnis erlangt hat, die personenbezogene Daten betrifft, für die der Auftraggeber verantwortlich ist, und unterstützt den Auftraggeber bei der Erfüllung seiner gesetzlichen Pflichten gemäß den geltenden Datenschutzgesetzen.

5.3 Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen trifft der Anbieter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Art. 32 DSGVO), um die fortlaufende Vertraulichkeit, Integrität, Verfügbarkeit und Widerstandsfähigkeit der Verarbeitungssysteme und -dienste sicherzustellen. Die vom Anbieter umgesetzten technischen und organisatorischen Maßnahmen findet der Auftraggeber in seinem Apotheken-Cockpit.

5.4 Auf Anweisung des Auftraggebers und soweit möglich, wird der Anbieter personenbezogene Daten gemäß den Anweisungen des Auftraggebers korrigieren, sperren oder löschen. Wenn sich eine betroffene Person direkt an den Anbieter wendet, um ihre Daten korrigieren, löschen oder sperren zu lassen, weist der Anbieter die betroffene Person an, sich unverzüglich nach Erhalt der Anfrage an den Verantwortlichen zu wenden.

5.5 Der Anbieter unterstützt den Auftraggeber bei der Einhaltung der Verpflichtungen gemäß Art. 32-36 DSGVO unter Berücksichtigung der Art der Verarbeitung und der dem Anbieter zur Verfügung stehenden Informationen. Soweit die erforderlichen Informationen dem Anbieter in zumutbarer Weise zur Verfügung stehen und der Auftraggeber nicht anderweitig Zugang zu den erforderlichen Informationen hat, unterstützt der Anbieter den Auftraggeber in angemessener Weise bei der Durchführung von Datenschutz-Folgenabschätzungen und der vorherigen Konsultation von Aufsichtsbehörden oder anderen zuständigen Datenschutzbehörden, soweit dies nach den geltenden Datenschutzgesetzen erforderlich ist.

- 5.6 Der Anbieter wird sich in angemessener Weise bemühen, vollständig zu kooperieren und alle Anweisungen, Richtlinien und Anordnungen der zuständigen Aufsichtsbehörde zu befolgen. Der Anbieter hat den Auftraggeber unverzüglich über etwaige Maßnahmen der zuständigen Aufsichtsbehörde zu unterrichten, sofern diese Maßnahmen die Datenverarbeitung von dem Anbieter für den Auftraggeber betreffen.
- 5.7 Der Anbieter führt ein Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DSGVO und stellt es dem Auftraggeber auf Anfrage zur Verfügung.
- 5.8 Der Anbieter informiert den Auftraggeber unverzüglich, wenn der Anbieter feststellt, dass bei der Verarbeitung personenbezogener Daten des Auftraggebers gegen geltende Datenschutzgesetze verstoßen wurde oder es zu einer Verletzung des Schutzes personenbezogener Daten gekommen ist bzw. der Anbieter den Verdacht einer solchen Verletzung hat, es sei denn dies ist dem Anbieter nach den anwendbaren Gesetzen oder aufgrund einer behördlichen Anordnung untersagt. Der Anbieter wird den Auftraggeber bei seinen Pflichten nach Art. 33, 34 DSGVO erforderlichenfalls in angemessener Weise unterstützen.

6. Unterauftragsverarbeiter

- 6.1 Der Auftraggeber erteilt dem Anbieter eine allgemeine Genehmigung gemäß Art. 28 Abs. 2 DSGVO zur Beauftragung von Unterauftragsverarbeitern zum Zwecke der Erbringung der Dienstleistungen.
- 6.2 Der Auftraggeber ermächtigt den Anbieter zur Beauftragung der **Anlage 1** zu diesem Vertrag aufgeführten Unterauftragsverarbeiter zum Zeitpunkt des Abschlusses dieses Vertrags.
- 6.3 Der Anbieter informiert den Auftraggeber vor der Ernennung eines neuen Unterauftragsverarbeiters. Nach der Benachrichtigung über die Absicht vom Anbieter, einen neuen Unterauftragsverarbeiter zu beauftragen, kann der Auftraggeber dieser Beauftragung widersprechen, indem er den Anbieter innerhalb von fünf (5) Werktagen nach Erhalt der Mitteilung vom Anbieter schriftlich per E-Mail an support@gesund.de benachrichtigt.
- 6.4 Wenn der Auftraggeber innerhalb von fünf (5) Werktagen nach Erhalt dieser Benachrichtigung den Anbieter schriftlich über (begründete) Einwände gegen die vorgeschlagene Ernennung informiert: (a) wird der Anbieter angemessene Anstrengungen unternehmen, um eine wirtschaftlich vertretbare Änderung bei der Erbringung der Dienstleistungen zu ermöglichen, die den Einsatz des vorgeschlagenen Unterauftragsverarbeiters vermeidet; und (b) wenn: (i) eine solche Änderung nicht innerhalb von dreißig (30) Werktagen nach Eingang der Mitteilung des Auftraggebers bei dem Anbieter vorgenommen werden kann; (ii) keine wirtschaftlich vertretbare Änderung möglich ist; und/oder (iii) der Auftraggeber es ablehnt, die Kosten für die vorgeschlagene Änderung zu tragen, kann jede Partei ungeachtet der Bestimmungen des Vertrags den Vertrag durch schriftliche Mitteilung an die andere Partei mit sofortiger Wirkung entweder vollständig oder in dem Umfang kündigen, in dem er sich auf die Dienstleistungen bezieht, die den Einsatz des vorgeschlagenen Unterauftragsverarbeiters erfordern.
- 6.5 Der Anbieter darf einen Unterauftragsverarbeiter nur beauftragen, sofern mit diesem eine Vereinbarung abgeschlossen wurde, die dem Unterauftragsverarbeiter ähnliche und in keiner Weise weniger schützende Verpflichtungen als die in diesem Vertrag festgelegten auferlegt.
- 6.6 Sofern der Anbieter einen Unterauftragsverarbeiter in einem Drittland beauftragt, stellt der Anbieter sicher, dass ein angemessenes Datenschutzniveau für die Übermittlung der personenbezogenen Daten an den Unterauftragsverarbeiter besteht oder geschaffen wird (z.B. durch den Abschluss von EU-Standardvertragsklauseln).

- 6.7 Der Anbieter ist in vollem Umfang für Datenschutzverstöße der Unterauftragsverarbeiter im Zusammenhang mit der Erbringung von Dienstleistungen verantwortlich und haftet gegenüber dem Auftraggeber in vollem Umfang für derartige Verstöße gemäß Art. 28 Abs. 4 S. 2 DSGVO.

7. Kontrollen durch den Auftraggeber

- 7.1 Der Anbieter gewährt dem Auftraggeber und seinen Beauftragten während der Laufzeit des Vertrags alle angeforderten Informationen und Zugriffsrechte unter strikter Einhaltung der Sicherheitsrichtlinien vom Anbieter, um die Einhaltung dieses Vertrags und der geltenden Datenschutzgesetze durch den Anbieter auf schriftliche Anfrage des Auftraggebers zu überprüfen.
- 7.2 Der Auftraggeber kann die Einhaltung der vereinbarten technischen und organisatorischen Maßnahmen (siehe Apotheken-Cockpit) durch den Anbieter in den Einrichtungen vom Anbieter nach angemessener schriftlicher Aufforderung einmal im Jahr überprüfen, was der Vertraulichkeit unterliegt.
- 7.3 Wenn und soweit der Auftraggeber Dritte mit der Durchführung eines Audits beauftragt, müssen diese Dritten an ähnliche und nicht weniger schützende Vertraulichkeitsverpflichtungen gebunden sein, wie sie in diesem Vertrag und dem Hauptvertrag vereinbart sind.
- 7.4 Der Auftraggeber erstattet dem Anbieter den Zeitaufwand für Vor-Ort-Audits zu den jeweils gültigen Sätzen für professionelle Dienstleistungen vom Anbieter.
- 7.5 Der Auftraggeber ist verpflichtet, den Anbieter unverzüglich über tatsächliche oder vermutete Verstöße, die während eines Audits festgestellt werden, zu informieren und Auskunft zu erteilen.

8. Pflichten bei Beendigung des Vertrags

- 8.1 Bei Beendigung des Vertrags aus irgendeinem Grund oder jederzeit auf schriftliche Aufforderung des Auftraggebers stellt der Anbieter die personenbezogenen Daten zum Herunterladen zur Verfügung oder gibt sie an den Auftraggeber zurück und/oder löscht oder vernichtet sicher und in Übereinstimmung mit den geltenden Datenschutzgesetzen alle Originale und Kopien der personenbezogenen Daten, es sei denn, dieser Vertrag oder die Datenschutzgesetze verlangen etwas anderes.
- 8.2 Auf schriftliche Anfrage des Auftraggebers stellt der Anbieter dem Auftraggeber unverzüglich eine schriftliche Bestätigung zur Verfügung, dass alle personenbezogenen Daten an den Auftraggeber zurückgegeben oder sicher vernichtet wurden.

9. Schlussbestimmungen

- 9.1 Dieser Vertrag kommt durch elektronischen Abschluss im Apotheken-Cockpit zustande. Änderungen und Ergänzungen dieses Vertrags bedürfen der Schriftform. Die elektronische Form ist hierfür ausreichend (§§ 126 Abs. 3, 126 a BGB).
- 9.2 Sollten einzelne Bestimmungen dieses Vertrags ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.
- 9.3 Dieser Vertrag unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist der Sitz vom Anbieter. Der Anbieter bleibt berechtigt, am allgemeinen Gerichtsstand des Auftraggebers zu klagen.

Anlage 1 – Genehmigte Unterauftragsverarbeiter

Folgende Unterauftragsverarbeiter gelten mit Abschluss dieses Vertrages als durch den Auftraggeber genehmigt:

Firma, Adresse	Ort der Datenverarbeitung	Auftrag/Art der Datenverarbeitung
Sendinblue SAS (Brevo) 106 boulevard Haussmann, 75008 Paris, Frankreich	EU	Versand von E-Mails im Rahmen der Online-Terminbuchung (Buchungsbestätigungen, Terminerinnerungen, Stornierungen, Benachrichtigungen an die Apotheke)