Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DS-GVO
zwischen

[.....]
[Name und Adresse der Apotheke]

als Verantwortlicher (hier bezeichnet als „Auftraggeber“)

und

der Alliance Healthcare Deutschland GmbH,

Solmsstraße 73, 60486 Frankfurt am Main,

als Auftragsverarbeiter (hier bezeichnet als „Auftragnehmer“)

Präambel

Der Auftraggeber möchte den Auftragnehmer mit den in § 2 genannten Leistungen beauftragen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DS-GVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung, deren Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

§ 1 Begriffsbestimmungen

In diesem Vertrag verwendete Begriffe, die in Art. 4, 9 und 10 DS-GVO definiert werden, sind im Sinne dieser gesetzlichen Definition zu verstehen.

§ 2 Vertragsgegenstand

(1) Der Auftragnehmer erbringt für den Auftraggeber die Dienstleistung Webshop-Service auf Grundlage der Vereinbarung über die Teilnahme am AHD Webshop-Service (nachfolgend: Hauptvertrag) sowie etwaiger Ergänzungsvereinbarungen. Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers, sofern der Auftragnehmer nicht durch das Recht der Union oder der Mitgliedsstaaten, dem er unterliegt, zu einer anderen Verarbeitung verpflichtet ist. Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus dem Hauptvertrag sowie aus der **Anlage 1** zu diesem Vertrag. Dem Auftraggeber obliegt die alleinige Beurteilung der Zulässigkeit der Datenverarbeitung gemäß Art. 6 Abs. 1 DS-GVO.

(2) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

(3) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden oder auf sonstige Weise in dessen Auftrag verarbeitet werden.

(4) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

(5) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der europäischen Union statt oder in einem anderen Drittland, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

§ 3 Art der verarbeiteten Daten, Kreis der betroffenen Personen

Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragnehmer Zugriff auf die in **Anlage 1** näher spezifizierten personenbezogenen Daten der ebenfalls in **Anlage 1** näher spezifizierten betroffenen Personen. Diese Daten umfassen die in **Anlage 1** aufgeführten und als solche gekennzeichneten besonderen Kategorien personenbezogener Daten.

§ 4 Weisungsrecht

(1) Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers erheben, nutzen oder auf sonstige Weise verarbeiten; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit. Statistische Daten ohne Personenbezug darf der Auftragnehmer auch zu eigenen Zwecken verarbeiten.

(2) Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in dokumentiertem elektronischem Format durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung), soweit Hauptvertrag oder dieser Vertrag es gestatten. Der Auftraggeber ist jederzeit zur Erteilung von Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten berechtigt.

(3) Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren und für die Dauer ihrer Geltung sowie anschließend für drei weitere volle Kalenderjahre aufzubewahren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen der Auftraggeberin an die Auftragnehmerin entstehen, bleiben unberührt.

(4) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 5 Schutzmaßnahmen des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird und gewährleistet, dass er alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DS-GVO, insbesondere mindestens die in **Anlage 2** aufgeführten Maßnahmen getroffen hat. Sofern auch besondere Kategorien personenbezogener Daten verarbeitet werden, trifft der Auftragnehmer zusätzlich die sich aus § 22 Absatz 2 BDSG ergebenden angemessenen und spezifischen Maßnahmen. Der Auftragnehmer legt auf Anforderung des Auftraggebers die näheren Umstände der Festlegung und Umsetzung der Maßnahmen offen. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Beim Auftragnehmer ist ein betrieblicher Datenschutzbeauftragter bestellt. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers hinterlegt.

(4) Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu nutzen oder auf sonstige Weise zu verarbeiten. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im folgenden Beschäftigte genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DS-GVO) und über die sich aus diesem Vertrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehren sowie mit der gebotenen Sorgfalt die Einhaltung der vorgenannten Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Beschäftigten und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

§ 6 Informationspflichten des Auftragnehmers

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder dokumentiertem elektronischen Format informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält soweit möglich folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;
b) eine Beschreibung der wahrscheinlichen Folgen der Verletzung und
c) eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(2) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Person(en), informiert hierüber den Auftraggeber und ersucht diesen um weitere Weisungen.

(3) Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.

(4) Der Auftragnehmer unterstützt den Auftraggeber erforderlichenfalls bei der Erfüllung der Pflichten des Auftraggebers nach Art. 33 und 34 DS-GVO in angemessener Weise (Art. 28 Abs. 3 S. 2 lit. f DS-GVO). Meldungen für den Auftraggeber nach Art. 33 oder 34 DS-GVO darf der Auftragnehmer nur nach vorheriger Weisung seitens des Auftraggebers gem. § 5 dieses Vertrags durchführen.

(5) Der Auftragnehmer und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DS-GVO enthält. Das Verzeichnis ist dem Auftraggeber auf Anforderung zur Verfügung zu stellen.

(6) Bei der Erstellung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO und ggf. bei der vorherigen Konsultation der Aufsichtsbehörden gemäß Art. 36 DS-GVO hat der Auftragnehmer im angemessenen Umfang mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

§ 7 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers. Hierfür kann er z. B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche, schriftliche oder elektronische Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind.

(3) Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

(4) Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung.

(5) Der Auftragnehmer weist dem Auftraggeber die Verpflichtung der Mitarbeiter nach § 5 Abs. 4 auf Verlangen nach.

§ 8 Einsatz von Subunternehmern

(1) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in **Anlage 3** genannten Subunternehmer durchgeführt. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt. Er setzt den Auftraggeber hiervon unverzüglich in Kenntnis. Der Auftragnehmer ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer hat bei der Einschaltung von Subunternehmern diese entsprechend den wesentlichen Regelungen dieser Vereinbarung zu verpflichten. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

(2) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

§ 9 Anfragen und Rechte betroffener Personen

(1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32 und 36 DS-GVO.

(2) Macht eine betroffene Person Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist die betroffene Person unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

§ 10 Haftung

(1) Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung. Der Auftragnehmer stimmt eine etwaige Erfüllung von Haftungsansprüchen mit dem Auftraggeber ab.

(2) Die Parteien stellen sich jeweils von der Haftung frei, wenn / soweit eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einer betroffenen Person eingetreten ist, verantwortlich ist. Im Übrigen gilt Art. 82 Absatz 5 DS-GVO.

(3) Sofern vorstehend nicht anders geregelt, entspricht die Haftung im Rahmen dieses Vertrages der des Hauptvertrages.

§ 11 Außerordentliches Kündigungsrecht

Der Auftraggeber kann den Hauptvertrag fristlos ganz oder teilweise kündigen, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DS-GVO oder sonstige anwendbare Datenschutzvorschriften vorsätzlich oder grob fahrlässig verletzt oder eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer sich den Kontrollrechten des Auftraggebers auf vertragswidrige Weise widersetzt.

§ 12 Beendigung des Hauptvertrags

(1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen.

(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht.

(3) Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

§ 13 Schlussbestimmungen

(1) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform oder eines dokumentierten elektronischen Formats. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

(3) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

(4) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Frankfurt am Main

Alliance Healthcare Deutschland GmbH

ppa.	ppa.
	
……	……
Tanja Wilcke	**Lena Schmidt**
Head of Marketing & Communications	**Leitung Marketing**
……..	……
Ort, Datum	**Unterschrift Auftraggeber**

Anlagen:

Anlage 1 – Beschreibung der betroffenen Personen/Betroffenengruppen sowie der besonders schutzbedürftigen Daten/Datenkategorien; Einbindung Drittanbieter

Anlage 2 – Technische und organisatorische Maßnahmen des Auftragnehmers

Anlage 3 – Genehmigte Subunternehmer

Anlage 1 – Beschreibung der betroffenen Personen/Betroffenengruppen sowie der besonders schutzbedürftigen Daten/Datenkategorien

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten; Einbindung Drittanbieter

Die Verarbeitung der Daten dient dem Zweck einer ordnungsgemäßen Durchführung der vertraglichen Beziehungen aus dem Service AHD Webshop, insbesondere für die Abwicklung von (Vor-)Bestellungen der Endkunden inkl. Rezept-Scanning, dem Bereitstellen von Kommunikationseinrichtungen für den Endkunden, z.B. ein Kontaktformular, der Verarbeitung von Apothekendaten inklusive der Mitarbeiterdaten des Auftraggebers im Backend (Einrichtungsassistent / Apotheker Login) der Apotheke und bei der Selbstpräsentation der Apotheke (z.B. Bilder des Apothekenteams, Anzeige von google Bewertungen) auf der Website.

Umfasst ist auch die Einbindung von Cookies von Drittanbietern zur Analyse des Nutzungsverhaltens sowie zur Ausspielung von Werbung. Die nachfolgenden Dienste werden durch die folgenden Drittanbieter in eigener Verantwortung gemäß den gegenüber den Nutzern der Website erteilten Datenschutzhinweisen verarbeitet:

- Facebook Pixel und Facebook Custom Audiences sowie Facebook Connect der Facebook Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Irland ("Facebook"; Mutterunternehmen: Facebook Inc., 1601 Willow Road, Menlo Park, CA 94025, USA)
- Google Ads DoubleClick, YouTube Videos und Google Analytics 4 (letzteres als Auftragsverarbeiter), Services der Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland, (Google).
- Bing Ads (inklusive Bing Universal Event Tracking, "UET"), einen Service der Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Irland ("Microsoft"),

Die Nutzer werden über ein vom Auftragnehmer ausgewählten Consent Banner über die Datenverarbeitung informiert und haben die Möglichkeit in das Setzen von Cookies und die Datenverarbeitung einzuwilligen.

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Kategorien betroffener Personen und folgender Datenarten/-kategorien:

Endkunden/Patienten des Auftraggebers:

Kommunikationseinrichtung: Name (Vor- und Nachname), Kontaktdaten, wie E-Mail-Adresse/Telefon, Informationen, die über das Nachrichtenfeld übermittelt werden, Protokolldateien, IP-Adresse.

Bei der (Vor-)Bestellung von Ware: Anrede, Name (Vor- und Nachname), Artikelname, die PZN der vorbestellten Ware, Kontaktdaten, wie E-Mail-Adresse/Telefon, Protokolldateien, IP-Adresse, sowie die sich daraus ergebenden Informationen über den Gesundheitszustand des Endkunden/Patienten und damit Gesundheitsdaten im Sinne von Art 9 Abs1. DSGVO. Bei der Lieferung nach Hause per Bote zusätzlich die Adressdaten. Bei der Vorbestellung rezeptpflichtiger Ware zusätzlich das Bild des Rezeptes.

Bei Einwilligung in das Setzen von Cookies werden Daten über das Nutzungsverhalten auf der Website erhoben.

Apothekendaten inklusive Mitarbeiterdaten des Auftraggebers

Bei der Nutzung des Apothekenbackend/Interface, Selbstpräsentation der Apotheke (z.B. google Bewertungen) , sowie für den Fall, dass der Auftraggeber den Auftragnehmer mit der Befüllung seines Google MyBusiness-Konto beauftragt: Verarbeitung des Namen der Mitarbeiter des Auftraggebers, IP-Adresse, Standortdaten, Öffnungszeiten, ggf. Paypal-ID-Nummer.

Anlage 2 – Technische und organisatorische Maßnahmen des Auftragnehmers

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)
   - **Zutrittskontrolle**
     Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden. Dies wird gewährleistet durch:
     - Zutrittskontrollsystem (z.B. Schlüssel, Magnetkarte, Chipkarte)
     - (Kontrollierte) Schlüssel / Schlüsselvergabe
     - Türsicherung (elektrische Türöffner usw.)
     - Videoüberwachung der Zugänge

- Besucherregistrierung durch Empfang
- Alarmanlage

- **Zugangskontrolle**
  Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und –verfahren benutzen. Dies wird gewährleistet durch:
  - Kennwortverfahren
  - Automatische Sperrmechanismen
  - Zwei-Faktor-Authentifizierung bei Remote-Zugriffen zu Wartungszwecken;
  - Verschlüsselung von Datenbanken und -trägern

- **Zugriffskontrolle**
  Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können. Dies wird gewährleistet durch:
  - Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte
  - Protokollierung und Auswertung von Zugriffen
  - Überprüfung der gewährten Zugriffsrechte auf Notwendigkeit

- **Trennungskontrolle**
  Maßnahmen, die getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, gewährleisten. Dies wird gewährleistet durch:
  - Mandantenfähigkeit

- **Pseudonymisierung /Verschlüsselung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)**
  Maßnahmen, die verhindern, dass Unbefugte die Einsicht in personenbezogene Daten erhalten. Dies wird gewährleistet durch:
  - Verschlüsselung des Speichermediums (z.B. Festplatte)
  - Verschlüsselung auf dem Transportwerg / Transportverschlüsselung
  - Pseudonymisierungs-/Anonymisierungsmechanismen (z.B. IP-Adress-Anonymisierung)

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)
   - **Weitergabekontrolle**
     Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Dies wird gewährleistet durch:
     - Speicher- und Transportverschlüsselung
     - Tunnelverbindung (= Virtual Private Network);
     - Elektronische Signatur
     - Spezieller Prozess zur Außerbetriebnahme eines Speichergerätes

   - **Eingabekontrolle**
     Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind. Dies wird gewährleistet durch:
     - Protokollierung

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DS-GVO)
   Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind: Dies wird gewährleistet durch:
   - Backup-Verfahren; Firewall/Virenschutz
   - Redundante Systeme
   - unterbrechungsfreie Stromversorgung (USV);
   - Notfallpläne

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- **Managementsysteme**:
  - Datenschutz-Management
  - Sensibilisierung Mitarbeiter zum Datenschutz
  - Benennung Datenschutzbeauftragter
  - Risikomanagement
  - Tätigkeitsbericht des Datenschutzbeauftragten
  - Incident-Response-Management

- **Datenschutzmechanismen:**
  - Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);

- **Auftragskontrolle:**
  - Regelmäßiges Datenschutz-Audit
  - Keine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

Anlage 3 – Genehmigte Subunternehmer

Folgende Subunternehmer wurden genehmigt:

- Mauve Mailorder Software GmbH & Co KG
  Steeler Wasserturm
  Laurentiusweg 83
  45276 Essen

- Caesar und Gustav Werbegentur
  Rotenbergstraße 39
  70190 Stuttgart

- IFEMEDI / Pharma Marketing Consulting
  Inhaber: Dr. oec. troph. Jörg Hüve
  Hopfenweg 44c
  26125 Oldenburg

- Emarsys Interactive Services GmbH
  Willi-Schwabe-Straße
  12489 Berlin