Docusign Envelope ID: BE46C8ED-7285-8316-8018-B652FDD29592

Vertrag über die Verarbeitung von personenbezogenen Daten im Auftrag

zwischen

dem Kunden des Auftragnehmers, welcher Bestellungen über den Online-Shop des Auftragnehmers aufgibt, also jede Apotheke oder sonstige juristische oder natürliche Person, die den Online-Shop des Auftragnehmers nutzt, registriert ist und diesem Auftragsverarbeitungsvertrag elektronisch zugestimmt hat. Die individuellen Kontaktdaten des Auftraggebers ergeben sich aus dem jeweiligen Kundenkonto im Online-Shop.

- Auftraggeber -

und

OTG Handels GmbH
Wolfener Str. 32
12681 Berlin

- Auftragnehmer -

Der Vertrag wird vom Auftraggeber elektronisch durch Setzen eines Häkchens beim Login zum Online-Shop angenommen. Mit dieser Zustimmung erkennt der Auftraggeber die Vertragsinhalte verbindlich an. Eine gesonderte handschriftliche Unterzeichnung durch den Kunden ist nicht erforderlich. Mit der Deaktivierung des Online-Shop-Kundenkontos endet der AVV nach Maßgabe der Ziff. 15 und 16.

1. Allgemeines

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i. S. d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

(2) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i. S. d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

2. Gegenstand des Auftrags

(1) Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in **Anlage 1** zu diesem Vertrag festgelegt. Dieser Vertrag erfasst ausschließlich die Speicherung, Verwaltung und technische Bereitstellung der Daten im Kundenkonto des Online-Shops einschließlich der hierfür erforderlichen Betriebs-, Wartungs- und Supportleistungen. Die Abgrenzung zur Bestellabwicklung und Herstellung ergibt sich aus Anlage 1 Nr. 1.

Docusign Envelope ID: BE46C8ED-7285-8316-8018-B652FDD29592

3. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher i. S. d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer.

(2) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen.

(3) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen können in Textform (z.B. E-Mail) erfolgen.

(4) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

(5) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

(6) Der Auftraggeber stellt für die Speicherung und Verwaltung im Online-Shop nur diejenigen personenbezogenen Daten bereit, die für die von ihm festgelegten Zwecke erforderlich sind. Er ist für die Rechtmäßigkeit dieser Verarbeitung und die Erfüllung seiner datenschutzrechtlichen Pflichten gegenüber den betroffenen Personen verantwortlich. Dies umfasst eine Rechtsgrundlage nach Art. 6 DSGVO sowie bei Gesundheitsdaten zusätzlich die Voraussetzungen einer Ausnahme nach Art. 9 Abs. 2 DSGVO einschließlich gegebenenfalls anwendbarer ergänzender Rechtsvorschriften und Geheimhaltungspflichten. Dieser Vertrag begründet selbst keine Rechtsgrundlage für die Verarbeitung oder Übermittlung der Daten. Die eigenen gesetzlichen Pflichten des Auftragnehmers bleiben unberührt.

4. Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet die von diesem Vertrag erfassten personenbezogenen Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und auf dokumentierte Weisung des Auftraggebers; dies gilt auch für Übermittlungen. Eine Verarbeitung ohne Weisung ist nur zulässig, soweit der Auftragnehmer hierzu durch das Recht der Union oder der Mitgliedstaaten, dem er unterliegt, verpflichtet ist. In diesem Fall teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich nach diesem Vertrag und den ergänzenden Weisungen des Auftraggebers. Abweichungen bedürfen der Zustimmung des Auftraggebers in Textform.

(2) Der Auftragnehmer verpflichtet sich, die Datenverarbeitung im Auftrag nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen.

(3) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung so lange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das

Docusign Envelope ID: BE46C8ED-7285-8316-8018-B652FDD29592

Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen. Eine Bestätigung rechtfertigt keine rechtswidrige Verarbeitung. Gesetzliche Ansprüche betroffener Personen, die Haftung nach Art. 82 DSGVO und der gesetzliche Innenausgleich nach Art. 82 Abs. 5 DSGVO bleiben unberührt.

5. Datenschutzbeauftragter des Auftragnehmers

(1) Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DSGVO benannt und gemäß den gesetzlichen Anforderungen qualifiziert hat. Der Auftragnehmer stellt dem Auftraggeber dessen Namen und Kontaktdaten bei Vertragsschluss in Textform oder im Online-Shop dauerhaft abrufbar zur Verfügung und informiert über Änderungen.

6. Meldepflichten des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen.

(2) Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann.

(3) Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen.

7. Mitwirkungspflichten des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO. Es gelten die Regelungen von Ziff. 11 dieses Vertrages.

(2) Der Auftragnehmer wirkt an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten durch den Auftraggeber mit. Er hat dem Auftraggeber die insoweit jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

(3) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

8. Kontrollbefugnisse

(1) Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer im erforderlichen Umfang zu kontrollieren.

(2) Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i. S. d. Absatzes 1 erforderlich ist.

Docusign Envelope ID: BE46C8ED-7285-8316-8018-B652FDD29592

(3) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Die Kontrolle ist auf den erforderlichen Umfang zu beschränken; Betriebsabläufe sowie die Sicherheit, Geschäftsgeheimnisse und Daten anderer Kunden sind angemessen zu berücksichtigen. Die Parteien gehen davon aus, dass eine reguläre Kontrolle grundsätzlich höchstens einmal jährlich erforderlich ist. Weitere erforderliche Kontrollen, insbesondere aufgrund eines Datenschutzvorfalls, wesentlicher Änderungen der Verarbeitung, begründeter Zweifel an der Einhaltung der Pflichten oder auf Verlangen einer Aufsichtsbehörde, bleiben unberührt. Der Auftraggeber teilt den Anlass einer zusätzlichen Kontrolle mit. In dringenden Fällen ist die Ankündigungsfrist entsprechend zu verkürzen; soweit der Kontrollzweck dies erfordert, kann eine vorherige Ankündigung entfallen.

(4) Der Auftragnehmer kann geeignete, aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen sowie geeignete Zertifizierungen zum Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen vorlegen. Der Auftraggeber berücksichtigt diese Nachweise bei der Beurteilung des erforderlichen Kontrollumfangs. Sie ersetzen eine erforderliche weitergehende Überprüfung einschließlich einer Vor-Ort-Kontrolle nicht einseitig. Die abschließende Entscheidung über Art und Umfang der erforderlichen Kontrolle verbleibt beim Auftraggeber unter Beachtung des Absatzes 3. Die Parteien stimmen die Durchführung ab; diese Abstimmung darf die Ausübung des Kontrollrechts nicht vereiteln oder unangemessen verzögern.

(5) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i. S. d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende geplante Maßnahmen vom Auftragnehmer zu informieren.

09. Unterauftragsverhältnisse

(1) Der Auftragnehmer ist berechtigt, die in der Anlage zu diesem Vertrag angegebenen Unterauftragnehmer für die Verarbeitung von Daten im Auftrag einzusetzen. Allein die Mitwirkung an der Bestellabwicklung oder Herstellung außerhalb dieses Vertrages macht ein Unternehmen nicht zum Unterauftragnehmer im Rahmen dieses Vertrages. Der Wechsel von Unterauftragnehmern oder die Beauftragung weiterer Unterauftragnehmer ist unter den in Absatz 2 genannten Voraussetzungen zulässig.

(2) Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Der Auftragnehmer wird den Auftraggeber im Falle eines geplanten Wechsels eines Unterauftragnehmers oder bei geplanter Beauftragung eines neuen Unterauftragnehmers rechtzeitig, spätestens aber 4 Wochen vor dem Wechsel bzw. der Neubeauftragung in Textform informieren („Information“). Der Auftraggeber hat das Recht, dem Wechsel oder der Neubeauftragung des Unterauftragnehmers unter Angabe einer Begründung in Textform binnen drei Wochen nach Zugang der „Information“ zu widersprechen. Der Widerspruch kann vom Auftraggeber jederzeit in Textform zurückgenommen werden. Im Falle eines Widerspruchs kann der Auftragnehmer das Vertragsverhältnis mit dem Auftraggeber mit einer Frist von mindestens 14 Tagen zum Ende eines Kalendermonats kündigen. Der Auftragnehmer wird bei der Kündigungsfrist die Interessen des Auftraggebers angemessen

Docusign Envelope ID: BE46C8ED-7285-8316-8018-B652FDD29592

berücksichtigen. Wenn kein Widerspruch des Auftraggebers binnen drei Wochen nach Zugang der „Information“ erfolgt, gilt dies als Zustimmung des Auftraggebers zum Wechsel bzw. zur Neubeauftragung des betreffenden Unterauftragnehmers. Die Information muss die Identität, die vorgesehene Tätigkeit und die Verarbeitungsorte einschließlich etwaiger Fernzugriffe so beschreiben, dass der Auftraggeber den Einsatz beurteilen kann. Ziff. 4 Abs. 2 gilt auch für Unterauftragnehmer. Im Falle eines rechtzeitigen Widerspruchs darf der betroffene Unterauftragnehmer die Daten des Auftraggebers bis zu einer Einigung oder der Beendigung des betroffenen Auftrags nicht verarbeiten.

(3) Der Auftragnehmer ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten gemäß Art. 37 DSGVO benannt hat, sofern der Unterauftragnehmer zur Benennung eines Datenschutzbeauftragten gesetzlich verpflichtet ist.

(4) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten.

(5) Der Auftragnehmer hat mit dem Unterauftragnehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat der Auftragnehmer dem Unterauftragnehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Auftraggeber und Auftragnehmer festgelegt sind. Dem Auftraggeber ist der Auftragsdatenverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

(6) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 8 dieses Vertrages) des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

(7) Nicht als Unterauftragsverhältnisse i. S. d. Absätze 1 bis 6 sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. 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 personenbezogener Daten zu gewährleisten.

10. Vertraulichkeitsverpflichtung

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet.

(2) Der Auftragnehmer hat seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut gemacht und zur Vertraulichkeit verpflichtet.

(3) Die Verpflichtungen der Beschäftigten nach Absatz 2 sind dem Auftraggeber auf Anfrage nachzuweisen.

Docusign Envelope ID: BE46C8ED-7285-8316-8018-B652FDD29592

11. Wahrung von Betroffenenrechten

(1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützen. Der Auftragnehmer hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.

(2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Einschränkung der Verarbeitung oder Löschung - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

(3) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer entstehen, bleiben unberührt.

12. Geheimhaltungspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten einschließlich der Tatsache des Abschlusses dieses Vertrages sowie seiner Inhalte, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

(3) Fordert eine Behörde / Organe der Rechtspflege berechtigt hier umfasste Daten vom Auftragnehmer heraus, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.

13. Technische und organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

(2) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als **Anlage 2** zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Voraus mit dem Auftraggeber abstimmen. Maßnahmen, die routinemäßig erfolgen (Software-Updates) oder die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt

Docusign Envelope ID: BE46C8ED-7285-8316-8018-B652FDD29592

werden. Der Auftraggeber kann einmal jährlich oder bei begründeten Anlässen eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

14. Anlagen

(1) Anlagen dieses Vertrages sind alle Anlagen, die zum Zeitpunkt des Vertragsschlusses erwähnt und enthalten sind.

(2) Später hinzugefügte oder geänderte Anlagen werden Vertragsbestandteil, wenn sie ausdrücklich auf diesen Vertrag Bezug nehmen und von den Parteien in Textform vereinbart werden. Die besonderen Änderungsregelungen nach Ziff. 9 und 13 bleiben unberührt.

(3) Dem vorliegenden Vertrag sind zum Zeitpunkt des Abschlusses beigelegt:

- **Anlage 1**: Gegenstand des Auftrags
- **Anlage 2**: Technische und organisatorische Maßnahmen

15. Vertragslaufzeit

(1) Der Vertrag beginnt mit der Eröffnung des Kundenkontos im Onlineshop des Auftragnehmers und endet mit der Deaktivierung dieses Kundenkontos.

16. Beendigung

(1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt.

17. Schlussbestimmungen

(1) Für Nebenabreden ist die Schriftform erforderlich.

(2) Sollten einzelne Teile dieses Vertrages unwirksam / undurchführbar oder vom Auftragnehmer gestrichen worden sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht. Anstelle der unwirksamen / undurchführbaren Regelung tritt eine solche, die gesetzeskonform ist und die die Parteien gewollt hätten, hätten sie im Vertragsabschlusszeitpunkt die unwirksame / undurchführbare Regelung bereits gekannt.

Berlin, 05.10.2026

Signiert von:
Petra Kienbaum
1B24A64FC079408...

Frau Petra Kienbaum
Geschäftsführerin
OTG Handels GmbH

Docusign Envelope ID: BE46C8ED-7285-8316-8018-B652FDD29592

Anlage 1 - Gegenstand des Auftrags
A: Nutzung des B2B-Online-Shops des Auftragnehmers

1. Gegenstand des Auftrages

Der Auftragnehmer ermöglicht dem Auftraggeber Bestelldaten in seinem Kundenkonto im Online-Shop des Auftragnehmers zu speichern und zu verwalten. Hierbei geht es vor allem um die Nachvollziehbarkeit von Versorgungen mit medizinischen Hilfsmitteln und um die Dokumentation der Patientenversorgung. Die vom Auftraggeber im Online-Shop eingegebenen Daten werden für ihn durch den Auftragnehmer gespeichert. Es wird darauf hingewiesen, dass die auf diese Weise dem Auftragnehmer zugeleiteten Daten auf Systemen gespeichert werden, die ihrerseits der routinemäßigen Wartung unterliegen und in diesem Zusammenhang vom Auftragnehmer oder dessen Unterauftragnehmern (siehe unten Punkt 6.) einsehbar sein können. Darüber hinaus kann der Auftragnehmer im Rahmen von Störungsbeseitigung, Wartung und sonstigen Serviceleistungen auf die Systeme des Auftraggebers zugreifen und erhält ggf. Einblick in dort hinterlegte personenbezogene Daten des Auftraggebers. Dieser Vertrag gilt nicht für die Daten, die für eine konkrete Bestellung an die OTG Handels GmbH zur Bestellabwicklung oder an den Hersteller zur Herstellung des Hilfsmittels übermittelt werden. Für diese Verarbeitung sind die OTG Handels GmbH und der Hersteller jeweils selbst verantwortlich, soweit sie deren Zweck und Ablauf eigenständig bestimmen. Die Speicherung und Verwaltung der Patienten- und Bestellhistorie im Kundenkonto bleibt davon getrennt und unterliegt weiterhin diesem Vertrag.

2. Dauer der Verarbeitung

Die durch den Auftraggeber übermittelten Daten werden so lange verarbeitet, wie der Auftraggeber das Online-Angebot nutzt. Der Auftraggeber hat selbst die Möglichkeit, personenbezogenen Daten jederzeit zu löschen.

3. Art und Zweck der Verarbeitung

Der Online-Shop des Auftragnehmers bietet dem Auftraggeber die Möglichkeit, personenbezogene Daten von Endkunden (Patienten) abzuspeichern und im Rahmen der Versorgung mit medizinischen Hilfsmitteln zu pflegen. Diese Verarbeitung dient ausschließlich der vom Auftraggeber veranlassten elektronischen Verwaltung und Dokumentation der Patientenversorgung und bisheriger Bestellungen. Die Datenerhebung beim Auftraggeber dient dessen fachgerechter Beratung und Versorgung des Endkunden mit medizinischen Hilfsmitteln. Der Auftraggeber bestimmt die Zwecke und ist für das Vorliegen einer Rechtsgrundlage nach Art. 6 DSGVO sowie bei Gesundheitsdaten zusätzlich einer anwendbaren Ausnahme nach Art. 9 Abs. 2 DSGVO verantwortlich. Ergänzende gesetzliche Voraussetzungen, insbesondere Geheimhaltungspflichten, sind zu beachten. Eine bestimmte Rechtsgrundlage oder Ausnahme wird durch diesen AVV nicht pauschal festgelegt. Der Auftragnehmer verarbeitet die Daten im Anwendungsbereich dieses Vertrages ausschließlich auf dokumentierte Weisung; Ziff. 4 Abs. 1 bleibt unberührt.

4. Arten personenbezogener Daten

Der Auftraggeber hat die Möglichkeit folgende Datenarten einzugeben:

- Name, Vorname
- Geburtsdatum
- Geschlecht
- Bestelldaten
- Angaben zu Leibdaten
- Ggf. Messdaten (Körpermaße)

Docusign Envelope ID: BE46C8ED-7285-8316-8018-B652FDD29592

- Adresse
- Versicherungsnummer
- Kontaktdaten (Telefon, E-Mail)
- Versicherungskasse

Die Verarbeitung von Geschäftskontaktdaten durch den Auftragnehmer für eigene Vertrags- und Abrechnungszwecke fällt nicht unter diesen AVV.

5. Kategorien betroffener Person
Kunden des Auftraggebers (Endverbraucher) und Kontaktdaten des Auftraggebers.

6. Unterauftragnehmer

Der Auftragnehmer hat mit seinen eingesetzten Unterauftragnehmern Auftragsverarbeitungsverträge geschlossen.

Name	Adresse	Tätigkeit innerhalb dieses AVV
Netigo GmbH	Fährstraße 1, 40221 Düsseldorf	Betrieb und Pflege des Online-Shops, soweit dies die Speicherung und Verwaltung der Daten im Kundenkonto betrifft.
AWS Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy, 1855 Luxemburg	Datenspeicherung für die vom AVV erfassten Shop-Funktionen.
SHORT CUTS GmbH design+kommunikation	Mehringdamm 55, 10961 Berlin	Bearbeitung und Pflege der Internetseite mit möglichem Zugriff auf die im Online-Shop gespeicherten personenbezogenen Daten. Zugriff nur im erforderlichen Umfang für diese Leistungen.

Wheel-IT AG (Josef-Reitert-Str. 4, 69190 Walldorf), Berkemann GmbH & Co. KG (Albin-May-Str. 3, 07937 Zeulenroda-Triebes) und SIC Sanivision Consulting GmbH (Spenglerstr. 8, 23556 Lübeck) übernehmen über Schnittstellen die für konkrete Bestellungen erforderlichen Daten aus dem Online-Shop und übermitteln sie an den Hersteller zur Herstellung der Produkte. Diese Tätigkeiten sind der in Nr. 1 abgegrenzten Bestellabwicklung und Herstellung zugeordnet und nicht der hier beauftragten Speicherung und Verwaltung der Patienten- und Bestellhistorie. Die Unternehmen sind für diese Tätigkeiten daher nicht als Unterauftragnehmer dieses AVV aufgeführt.

Docusign Envelope ID: BE46C8ED-7285-8316-8018-B652FDD29592

Anlage 2 - Technische und Organisatorische Maßnahmen

1. Einleitung

Die OTG Handels GmbH legt großen Wert auf die Einhaltung gesetzlicher Regelungen zum Datenschutz. Der Schutz personenbezogener Daten und der Privatsphäre von Kunden, Lieferanten, Mitarbeitern und sonstigen Dienstleistern / Vertragspartnern ist uns sehr wichtig. Technische und organisatorische Maßnahmen sollen dies sicherstellen. Die folgenden Angaben beziehen sich auf personenbezogene Daten, die durch unser Unternehmen verarbeitet werden und stellen einen Überblick über die eingesetzten Maßnahmen zur Gewährleistung des Datenschutzes dar. Sie dienen als Basis der Beschreibung der technischen und organisatorischen Maßnahmen gem. Art. 32 EU-DSGVO.

2. Vertraulichkeit und Geltungsbereich

Dieses Dokument ist vertraulich zu behandeln. Es ist vom Empfänger gegenüber unrechtmäßiger Kenntnis bzw. Einsichtnahme Dritter zu schützen.

3. Datenschutzrelevante Maßnahmen

a. Richtlinien

Um allen Mitarbeitern Dokumente zur Verfügung zu stellen, in welchen die wichtigsten Vorgaben zu Datenschutz und Informationssicherheit zusammengefasst sind, wurden entsprechende Richtlinien entwickelt. Diese informieren über Sinn und Zweck des Datenschutzes und stellen die wichtigsten Regeln und Grundprinzipien des Datenschutzes und der Informationssicherheit dar. Sie gelten für alle Mitarbeiter und basieren auf der, von der Geschäftsführung erlassenen, Leitlinie zu Datenschutz und Informationssicherheit.

b. Sensibilisierung der Mitarbeiter

Alle Mitarbeiter der OTG Handels GmbH wurden zu den Grundsätzen des Datenschutzes und der Informationssicherheit geschult und werden durch regelmäßige Schulungen und andere Awareness-Maßnahmen fortlaufend sensibilisiert. Alle Mitarbeiter haben eine Verschwiegenheitserklärung zu Datenschutz und Informationssicherheit unterschrieben.

c. Externe Stellen

Sollte der Auftragnehmer personenbezogene Daten im Rahmen der Auftragsverarbeitung an externe Stellen übermitteln oder erhalten, wird der vorgesehene Auftragsverarbeitungsvertrag zwischen Auftraggeber und Auftragnehmer abgeschlossen.

Auch andere Übermittlungen personenbezogener Daten im Rahmen der Geschäftsabwicklung erfolgen unter Berücksichtigung des Datenschutzes.

d. Betroffenenrechte

Die Rechte der Betroffenen (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch und Widerruf) werden wie gesetzlich gefordert gewahrt und entsprechend umgesetzt.

Docusign Envelope ID: BE46C8ED-7285-8316-8018-B652FDD29592

e. Betrieblicher Datenschutzbeauftragter

Ein betrieblicher Datenschutzbeauftragter wurde gem. Art. 37 EU-DSGVO schriftlich bestellt. Der Datenschutzbeauftragte wirkt auf die Einhaltung der gesetzlichen Vorschriften im Unternehmen hin. Entsprechend der EU-DSGVO verfügt der Datenschutzbeauftragte über eine unabhängige organisatorische Stellung und unterliegt bei der Ausführung seiner Aufgaben nicht den Weisungen der zu kontrollierenden Organisationseinheiten. Er führt die Sensibilisierung der Mitarbeiter bezüglich der Themen Datenschutz und Informationssicherheit durch. Zu seinen Aufgaben zählen außerdem die in unregelmäßigen Abständen stattfindenden Datenschutzprüfungen innerhalb der OTG Handels GmbH und die Beratung zu datenschutzrelevanten Themen.

4. Technische und organisatorische Maßnahmen

a. Zutrittskontrolle

Beim Auftragnehmer erfolgt eine Zutrittskontrolle zu den Betriebsgebäuden über ein manuelles Schließsystem mit Sicherheitsschlössern. Die Ausgabe der Schlüssel erfolgt nur an den notwendigen Personenkreis. In einem Schlüsselverzeichnis werden alle vorhandenen und sich im Umlauf befindenden Schlüssel protokolliert. Nach Wegfall der Erforderlichkeit zieht man die Schlüssel umgehend ein. Zutritt zu sensiblen Gebäudeteilen/Räumen (z.B. Technikräume) erhält nur ein eingeschränkter Personenkreis. Die Geschäftsräume der OTG-Handels GmbH befinden sich innerhalb eines geschossenen Gewerbegebietes, welches außerhalb der Geschäftszeiten verschlossen ist (Zufahrtsstraßen mit Schranken).

b. Zugangskontrolle zu IT-Systemen

Zur Kontrolle des Zugangs zu den IT-Systemen verfügt jeder Mitarbeiter über ein Benutzerprofil, Benutzername und Passwort sind für den Login notwendig. Die eingebundene Passwortrichtlinie enthält Sicherheitsvorgaben bzgl. der Frist der Passwortgültigkeit, der Passwortlänge und Komplexität und verbotene Passwörter. Die firmeneigenen Rechner sperren sich nach 10 Minuten Inaktivität automatisch. Eine erneute Passworteingabe durch den Nutzer ist notwendig.

Alle IT-Systeme mit dazugehöriger Hard- und Software werden von der IT-Abteilung verwaltet. Ein Firewall- und Virenschutz ist durchgängig installiert. Für externe Zugriffe wird eine VPN-Verbindung genutzt. Das WLAN ist nur für firmeneigene Geräte zugänglich. Für die Verwaltung der firmeneigenen Mobilgeräte (Smartphone, Tablet usw.) kommt eine Mobile-Device-Managementsoftware zum Einsatz.

c. Zugriffskontrolle

Individuelle Berechtigungsprofile innerhalb der unterschiedlichen Anwendungen gewährleisten, dass der berechtigte Benutzer ausschließlich auf die der Berechtigung unterliegenden Daten zugreifen kann. Nur Systemadministratoren, welche in ihrer Anzahl auf ein Minimum reduziert sind, können Benutzerprofile anlegen oder ändern. Berechtigungen werden nach einem vorgeschriebenen Prozess, mit entsprechenden Freigaben, vergeben. Die Daten auf den firmeneigenen Notebooks sind verschlüsselt. Sämtliche Datenträger werden sicher aufbewahrt. Es erfolgt eine datenschutzgerechte Entsorgung bzw. Vernichtung von Papierunterla-

Docusign Envelope ID: BE46C8ED-7285-8316-8018-B652FDD29592

gen, Festplatten, Computern und sonstigen elektronischen Datenträgern. Die Inhalte von Datenträger bzw. IT-Geräten, die den Benutzer wechseln oder anderweitig wiederverwend werden sollen, werden vorher entsprechend gelöscht.

d. Weitergabekontrolle

In der Regel gibt es keine Transporte von physischen Datenträgern. Sollte dies notwendig sein, findet eine sorgfältige Auswahl von Transportverpackung, -weg, -mittel und Personal statt. Datenübertragung erfolgt innerhalb des Unternehmens über LAN, WLAN, Internet oder E-Mail. Die firmeninterne E-Mail-Übertragung ist verschlüsselt. Verschlüsselt sind auch Übertragungen zu verbundenen Unternehmen auf Basis von VPN-Verbindungen. Beim Verbinden externer Rechner mit dem Firmennetz wird ein VPN-Zugang hergestellt.

Personenbezogene Daten werden bei Weitergabe innerhalb des Unternehmens möglichst anonymisiert oder pseudonymisiert. Bei Verschrottung, Veräußerung oder Fremdverwendung vormals firmengenutzter Hardware werden die Datenträger so gelöscht, dass keine Weiterverwendung von Daten durch Dritte erfolgen kann.

e. Eingabekontrolle

Die Benutzer können, soweit es das System ermöglicht, nur Eingaben oder Veränderungen vornehmen, die mit ihrem Berechtigungsprofil übereinstimmen, eine entsprechende Protokollierung kann erfolgen.

f. Auftragskontrolle

Bei der Auftragsverarbeitung schließt man den vorgesehenen Auftragsverarbeitungsvertrag ab, wobei die andere Vertragspartei sorgfältig ausgewählt wird. Gleiches gilt bei der Auswahl von Subauftragsnehmern. Nach Beendigung des Auftrags werden nicht mehr benötigte personenbezogene Daten, ggf. unter Beachtung von Archivierungsvorschriften, gelöscht.

g. Verfügbarkeitskontrolle

Das Rechenzentrum, welches sich bei einem beauftragten Dienstleister befindet, verfügt über angemessene Sicherheitsvorkehrungen, insbesondere werden folgende Punkte umgesetzt:

- Beachtung baulicher Mindestanforderungen (Doppelboden, Türen, Brandwiderstandsklasse F90 für Bauelemente, Kabel usw.)
- Brandmeldeanlage mit Brandfrüherkennung
- Brandvermeidungsanlage OxiReduct (Sauerstoffreduktion)
- Redundante, unterbrechungsfreie Stromversorgung
- Temperaturüberwachung & Doppelbodenklimatisierung
- Leckage-Sensoren zur Feuchtigkeits- und Wasserüberwachung
- Automatische Status- und Alarmmeldung
- Einbruchmeldeanlage (VdS Klasse C)
- Videoüberwachung mit Aufzeichnung
- Verschließbare Räume
- Verschließbare Rack-Schränke

Die Datensicherung wird durch ein regelmäßiges Backup-Verfahren gewährleistet bzw. werden redundante Systeme (RAID, NAS) eingesetzt. Darüber hinaus steht für den Notfall ein zweites, räumlich getrenntes und gespiegeltes Rechenzentrum am Standort zur Verfügung.

Docusign Envelope ID: BE46C8ED-7285-8316-8018-B652FDD29592

h. Trennungskontrolle

Durch den Einsatz von individuellen Benutzerprofilen, eines mandantenfähigen Systems, der Trennung von Buchungskreisen, welche nur mit entsprechender Berechtigung erreichbar sind und insgesamt zweckgebundene Berechtigungen für getrennte Aufgabenbereiche, wird die Trennungskontrolle gewährleistet. Darüber hinaus sind das Entwicklungs-, Test- und Produktivsystem strikt voneinander getrennt.

5. Abschluss

Alle genannten technischen und organisatorischen Maßnahmen unterliegen einer gewissen Weiterentwicklung bzw. dem technischen Fortschritt. Die genannten Maßnahmen stellen den aktuellen Stand der Technik dar und werden künftig weiterentwickelt. Dabei wird das Sicherheitsniveau bezüglich des Datenschutzes und der Datensicherheit nicht verringert.

Berlin, 05.10.2026