

# Vereinbarung zur Auftragsdatenverarbeitung

zwischen

---

Firma

---

Name

---

Straße – Hausnummer

---

PLZ - Wohnort

nachstehend Auftraggeber (Verantwortlicher) genannt

und

Hecht Contactlinsen GmbH

Dorfstraße 2-4

79280 Au

nachstehend Auftragnehmer (Auftragsverarbeiter) genannt

## Gegenstand und Dauer des Auftrags

- (1) Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: Fertigung von formstabilen und weichen Kontaktlinsen, Anbieten und Liefern von Handelswaren, Unterstützung und Beratung bei Fragen zur Produkthanwendung, Anbieten von Fortbildungsveranstaltungen sowie Verkaufsunterstützung (Aktionen, Konzepte, Software).
- (2) Der Auftrag wird auf unbestimmte Zeit geschlossen und ist jederzeit kündbar.

## Auftragsinhalt

- (1) Art und Zweck der vorgesehenen Verarbeitung der Daten

Für die unter „Gegenstand und Dauer des Auftrags“ genannten Aufgaben werden dem Auftragnehmer vom Auftraggeber bestimmte Arten personenbezogener Daten übermittelt.

### Fertigung und Lieferung von Kontaktlinsen

Für die Auftrags Erfüllung sind Angaben von technischen Parametern der herzustellenden Kontaktlinsen erforderlich. Auf Wunsch können im Rahmen der Auftragsabwicklung persönliche Daten (z.B. Kommission) angegeben werden. Für die Herstellung einer Sonderanfertigung fordert die Medizin-Produkte-Richtlinie (MDR) die Ausfertigung einer Erklärung gemäß Anhang XIII Abschnitt 1, die dem durch seinen Namen, ein Akronym oder einen numerischen Code identifizierbaren Patienten oder Anwender zur Verfügung gestellt wird. Eine "Sonderanfertigung" bezeichnet ein Produkt, das nur für einen einzigen Patienten bestimmt ist, um ausschließlich dessen individuellen Zustand und dessen individuellen Bedürfnissen zu entsprechen. Hierzu muss bei der Bestellung der Patientennamen angegeben werden.

### Unterstützung und Beratung bei Fragen zur Produkthanwendung

Bei der Beratung und Unterstützung zur Produkthanwendung werden personenbezogene Daten zur Erfüllung der Beratungsleistung benötigt. Dies ist nur dann der Fall, wenn sich die Beratung auf einen konkreten Kontaktlinsen-Träger bezieht. In diesem Fall sind mindestens die Refraktionswerte, die topographischen Daten, Indikationen und Kontraindikationen sowie allgemeine Informationen zum

Hornhautzustand des betreffenden Auges erforderlich. Bei Bedarf können diese Daten dem Auftragnehmer auch in elektronischer Form zur Verfügung gestellt werden. Diese Daten werden durch den Auftragnehmer ausschließlich zur Erfüllung der hier genannten Dienstleistung verwendet und konform mit der DSGVO behandelt.

#### **Anbieten und Liefern von Handelswaren**

Neben der Herstellung und Lieferung von Kontaktlinsen stellt der Auftragnehmer ein umfangreiches Angebot an Handelswaren zur Verfügung. Zur Auftragserfüllung sind Angaben zu Artikeln, Stückzahlen und gewünschten Lieferterminen erforderlich. Für die Verarbeitung dieser Daten gelten die in dieser Vereinbarung genannten Rechte und Pflichten.

#### **Anbieten von Fortbildungsveranstaltungen**

Der Auftragnehmer bietet verschiedene Seminare und Fortbildungsveranstaltungen an. Um eine größtmögliche Patientensicherheit gewährleisten zu können, koppelt der Auftragnehmer in Ausnahmefällen die Teilnahme an einer Veranstaltung mit der Bestellmöglichkeit für bestimmte Produktgruppen (z.B. Orthokeratologie). Der Auftraggeber erlaubt dem Auftragnehmer, die Daten besuchter Seminare oder Fortbildungsveranstaltungen für die oben genannten Ausnahmen und zur Dokumentation der Kundenhistorie zu speichern. Auch für die Verarbeitung dieser Daten gelten die in dieser Vereinbarung genannten Rechte und Pflichten.

#### **Verkaufsunterstützung**

Weiterhin werden vom Auftragnehmer verschiedene Aktionen und Konzepte zur Verkaufsunterstützung angeboten. Der Auftraggeber erlaubt nach Rücksprache und Einwilligung dem Auftragnehmer, diese Daten für Marketingaktivitäten zu verwenden. Für die Verarbeitung dieser Daten gelten die in dieser Vereinbarung genannten Rechte und Pflichten.

#### **Web-Angebot und Newsletter**

Das Web-Angebot des Auftragnehmers wird als zusätzliche Serviceleistung (Bereitstellung von Vorlagen und Informationsmaterial) und für den Informationsaustausch zur Verfügung gestellt. Zudem bietet der Auftragnehmer einen Email-Newsletter an. Die Zustellung des Newsletters kann jederzeit durch den Auftraggeber widerrufen werden. Dies gilt auch für Anmeldungen vor dem 25.5.2018. Für die Verarbeitung dieser Daten gelten die in dieser Vereinbarung genannten Rechte und Pflichten. Ergänzende datenschutzrelevante Hinweise sind in unserer Datenschutzerklärung enthalten (<http://www.hecht-kontaktlinsen.de/index.php/datenschutz>).

Die Durchführung der vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

### (2) Art der Daten

Gegenstand der Verarbeitung sind folgende Kategorien:

- Kommunikationsdaten (z.B. Telefon, Email, Adressdaten)
- Vertragsabrechnungs- und Zahlungsdaten
- Vertragsstammdaten
- Kundenhistorie
- Planungs- und Steuerungsdaten
- Optische und gesundheitsbezogene Daten (z.B. Refraktionsdaten, Topographiedaten) oder andere persönliche Merkmale, um einen individuellen Auftrag umsetzen zu können.

### (3) Kategorien der betroffenen Personen

- Kunden des Auftraggebers

- Endverbraucher des Auftraggebers
- Interessenten des Auftraggebers
- Beschäftigte des Auftraggebers
- Personenstammdaten

### **Technische und organisatorische Maßnahmen**

- (1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
- (2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c) und 32 DSGVO insbesondere in Verbindung mit Art. 5 DSGVO zu gewährleisten. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.
- (3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

### **Berichtigung, Einschränkung und Löschung der Daten**

- (1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit sich eine betroffene Person diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
- (2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

### **Qualitätssicherung und sonstige Pflichten des Auftragnehmers**

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 32 DSGVO; insofern gewährleistet er insbesondere die Einhaltung der folgenden Vorgaben:

- a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt. Als Datenschutzbeauftragter ist beim Auftragnehmer Herr Richard Gertis, Bergstr. 11, 79312 Emmendingen, bestellt.
- b) Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die

Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

- c) Der Auftragnehmer gewährleistet die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 und 32 DSGVO.
- d) Auftraggeber und Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- e) Der Auftragnehmer hat den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde zu informieren, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
- f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

### **Unterauftragsverhältnisse**

- (1) Als Unterauftragsverhältnis im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/ Transportleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
- (2) Die Auslagerung auf Unterauftragnehmer in Drittländer oder der Wechsel der bestehenden Unterauftragnehmer ist zulässig, soweit sie zur Vertragserfüllung dienen und der Auftragnehmer mit dem Unterauftragsnehmer geeignete Maßnahmen zur Einhaltung der Datenschutz-Grundverordnung veranlasst hat.
- (3) Die Auslagerung auf einen Unterauftragnehmer findet bei der Bestellung und Produktion weicher torischer Kontaktlinsen des Typs DT statt. Diese Kontaktlinsen werden durch die Medilens-Säntis AG hergestellt. Für die Auftragserfüllung sind Angaben zu technischen Parametern der herzustellenden Kontaktlinsen, die Auftragsnummer und der Kundename erforderlich.
- (4) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Auftraggebers.

### **Kontrollrechte des Auftraggebers**

- (1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer auf eigene Kosten Überprüfungen vorzunehmen oder Überprüfungen durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.
- (2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem

Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

- (3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann durch aktuelle Testate, Berichte oder Berichtsauszüge des Datenschutzbeauftragten erfolgen.
- (4) Für die Durchführung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

### **Mitteilung bei Verstößen des Auftragnehmers**

- (1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen und Datenschutz-Folgeabschätzungen. Hierzu gehören u.a.
  - a) Die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen.
  - b) Die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden.
  - c) Die Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevanten Informationen unverzüglich zur Verfügung zu stellen.
  - d) Die Unterstützung des Auftraggebers für dessen Datenschutzfolgeabschätzung.
  - e) Die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.
- (2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

### **Weisungsbefugnis des Auftraggebers**

- (1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).
- (2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

### **Löschung und Rückgabe von personenbezogenen Daten**

- (1) Kopien und Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungsfristen vorzuhalten sind.
- (2) Nach Abschluss der vereinbarten Arbeiten oder bereits nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände,

die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten.

- (3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

### Haftung

Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

### Schlussbestimmungen

- (1) Beide Vertragspartner sind verpflichtet, über die Vorschriften des Datengeheimnisses hinaus auch alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse, insbesondere von Geschäftsgeheimnissen und Datensicherungsmaßnahmen, vertraulich zu behandeln. Diese Verpflichtungen bestehen auch nach Beendigung des Vertragsverhältnisses fort.
- (2) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

---

Ort, Datum

79280 Au, den 14.06.2018

---

Ort, Datum



---

Stefan Muckenhirn, Geschäftsführer  
Hecht Contactlinsen GmbH  
Dorfstraße 2-4  
79280 Au