

# Auftragsverarbeitung personenbezogener Daten- HealthyCodes GmbH - V 1.1

Durch den Erhalt von Produkten oder Dienstleistungen des Auftragnehmers (Healthy Codes GmbH) sowie durch Ihre elektronische Zustimmung im Rahmen des Bestellprozesses erklären Sie, der Auftraggeber, verbindlich Ihr Einverständnis mit den Bestimmungen dieser Vereinbarung zur Auftragsverarbeitung personenbezogener Daten.

## 1. Einleitung, Geltungsbereich, Definitionen

- Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und -nehmer (im Folgenden „Parteien“ genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.
- Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer („Subunternehmer“) personenbezogene Daten des Auftraggebers in dessen Auftrag verarbeiten.
- In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung („DSGVO“) zu verstehen. In diesem Sinne ist der Auftraggeber der „Verantwortliche“, der Auftragnehmer der „Auftragsverarbeiter“. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

## 2. Gegenstand und Dauer der Verarbeitung

### 2.1. Gegenstand

Die Verarbeitung beruht auf dem zwischen den Parteien bestehenden AGBs.

### 2.2. Dauer

Die Verarbeitung beginnt mit der Bestellung des Kunden über unsere Website, sobald der Kunde den Plänen zustimmt und die Allgemeinen Geschäftsbedingungen, einschließlich dieser Datenschutzvereinbarung, akzeptiert. Die Verarbeitung erfolgt auf unbestimmte Zeit bis zur Kündigung dieses Vertrags oder des AGB durch eine der Parteien.

---

**Healthy Codes GmbH**

Am Kartoffelgarten 14,  
81671 München,  
Deutschland

**Geschäftsführer:**

Emad Ahmadi

**Gerichtsstand:** München

HRB 290591

VAT-ID: DE367004887

**Olinda Zweigniederlassung**

Deutschland

DBO 1001 0123 0712 3061

88

QNT0DEB2XXX

### 3. Art, Zweck und Betroffene der Datenverarbeitung

#### 3.1. Art der Verarbeitung

Die Verarbeitung ist folgender Art: Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung von Daten

#### 3.2. Zweck der Verarbeitung

Der zugrundeliegende Zweck der Verarbeitung ist in der Leistungsbeschreibung die AGB geregelt.

#### 3.3. Art der Daten

Es werden folgende Daten verarbeitet:

- Anrede
- Kommunikationsdaten
- Vor-und Zuname
- E-Mail-Adresse
- Adresse,
- Handynummer und Telefonnummer
- Verhaltensdaten
- Gesundheitsdaten (z. B. Informationen über Verschreibungen, in der Apotheke gekaufte Medikamente, Medikationsplan und andere gesundheitsbezogene Informationen)

#### 3.4. Kategorien der betroffenen Personen

Von der Verarbeitung betroffen sind:

- Kunden des Auftraggebers
- Interessenten des Auftraggebers
- Mitarbeiter des Auftraggebers

---

**Healthy Codes GmbH**

Am Kartoffelgarten 14,  
81671 München,  
Deutschland

**Geschäftsführer:**

Emad Ahmadi

**Gerichtsstand:** München

HRB 290591

VAT-ID: DE367004887

**Olinda Zweigniederlassung**

Deutschland

DBO 1001 0123 0712 3061

88

QNT0DEB2XXX

#### 4. Pflichten des Auftragnehmers

- Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Hiervon unberührt bleibt das Recht des Auftragnehmers, ihm vom Auftraggeber übermittelte Daten des Auftraggebers, aus denen jeglicher Personenbezug vollständig und dauerhaft entfernt wird, für eigene non-exklusiv für eigene Geschäftszwecke kostenlos für unbestimmte Zeit weltweit zu nutzen und zu verwerten.
- Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.
- Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.
- Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.
- Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.
- Im Zusammenhang mit der beauftragten Verarbeitung unterstützt der Auftragnehmer den Auftraggeber soweit erforderlich bei der Erfüllung seiner datenschutzrechtlichen Pflichten, insbesondere bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten, bei Durchführung der Datenschutzfolgeabschätzung und einer notwendigen Konsultation der Aufsichtsbehörde. Die erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.
- Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.
- Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.

**Healthy Codes GmbH**Am Kartoffelgarten 14,  
81671 München,  
Deutschland**Geschäftsführer:**

Emad Ahmadi

**Gerichtsstand:** München

HRB 290591

VAT-ID: DE367004887

**Olinda Zweigniederlassung**

Deutschland

DBO 1001 0123 0712 3061

88

QNT0DEB2XXX

- Soweit gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Es ist sicherzustellen, dass für den Beauftragten keine Interessenskonflikte bestehen. In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten wenden. Der Auftragnehmer teilt dem Auftraggeber unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit oder begründet, weshalb kein Beauftragter bestellt wurde. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer dem Auftraggeber unverzüglich mit.
- Die Auftragsverarbeitung personenbezogener Daten des Auftraggebers erfolgt ausschließlich innerhalb der EU oder des EWR.

#### 4. Sicherheit der Verarbeitung

- Die im Anhang 1 beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum. Die Beschreibung der Maßnahmen muss so detailliert erfolgen, dass für einen sachkundigen Dritten allein aufgrund der Beschreibung jederzeit zweifelsfrei erkennbar ist, was das geschuldete Minimum sein soll. Ein Verweis auf Informationen, die dieser Vereinbarung oder ihren Anlagen nicht unmittelbar entnommen werden können, ist nicht zulässig.
- Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftragnehmer unverzüglich umzusetzen. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.
- Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.
- Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.
- Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.
- Der Auftraggeber gestattet zum Zwecke der Durchführung dieser Auftragsverarbeitungsvereinbarung die Verarbeitung von Daten in Privatwohnungen. Soweit eine solche Verarbeitung erfolgt, ist vom Auftragnehmer sicherzustellen, dass dabei ein diesem Vertrag entsprechendes Niveau an Datenschutz und Datensicherheit aufrechterhalten wird und die in

---

**Healthy Codes GmbH**Am Kartoffelgarten 14,  
81671 München,  
Deutschland**Geschäftsführer:**

Emad Ahmadi

**Gerichtsstand:** München

HRB 290591

VAT-ID: DE367004887

**Olinda Zweigniederlassung**

Deutschland

DBO 1001 0123 0712 3061

88

QNT0DEB2XXX

diesem Vertrag bestimmten Kontrollrechte des Auftraggebers uneingeschränkt auch in den betroffenen Privatwohnungen ausgeübt werden können. Die Verarbeitung von Daten im Auftrag mit Privatgeräten ist unter keinen Umständen gestattet.

- Dedizierte Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden Verwaltung. Sie sind jederzeit angemessen aufzubewahren und dürfen unbefugten Personen nicht zugänglich sein. Ein- und Ausgänge werden dokumentiert.

## 6. Regelungen zur Berichtigung, Löschung und Sperrung von Daten

- Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren.
- Den entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit und auch über die Beendigung dieses Vertrages hinaus Folge leisten.

## 7. Unterauftragsverhältnisse

- Die Beauftragung von Subunternehmern ist nur mit schriftlicher Zustimmung des Auftraggebers im Einzelfall zugelassen. Der Auftragnehmer benötigt keine Einwilligung des Auftragsgebers für den Einsatz von Subunternehmern, die nur Betriebsdaten des Auftraggebers verwenden, die keine personenbezogenen Informationen enthalten.
- Die erlaubte Verarbeitung ist nur zulässig, wenn dem Subunternehmer vertraglich mindestens Datenschutzpflichten auferlegt wurden, die den in diesem Vertrag vereinbarten vergleichbar sind. Der Auftraggeber erhält auf Verlangen Einsicht in die relevanten Verträge zwischen Auftragnehmer und Subunternehmer.
- Die Rechte des Auftraggebers müssen auch gegenüber dem Subunternehmer wirksam ausgeübt werden können. Insbesondere muss der Auftraggeber berechtigt sein, jederzeit in dem hier festgelegten Umfang Kontrollen auch bei Subunternehmern durchzuführen oder durch Dritte durchführen zu lassen.
- Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind eindeutig voneinander abzugrenzen.
- Eine weitere Subbeauftragung durch den Subunternehmer ist nicht zulässig.
- Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.
- Die Weiterleitung von im Auftrag verarbeiteten Daten an den Subunternehmer ist erst zulässig, wenn sich der Auftragnehmer dokumentiert davon überzeugt hat, dass der Subunternehmer seine

Healthy Codes GmbH  
Am Kartoffelgarten 14,  
81671 München,  
Deutschland

Geschäftsführer:  
Emad Ahmadi

Gerichtsstand: München  
HRB 290591  
VAT-ID: DE367004887

Olinda Zweigniederlassung  
Deutschland  
DBO 1001 0123 0712 3061  
88  
QNT0DEB2XXX

Verpflichtungen vollständig erfüllt hat. Der Auftragnehmer hat dem Auftraggeber die Dokumentation unaufgefordert vorzulegen.

- Die Beauftragung von Subunternehmern, die Verarbeitungen personenbezogener Daten im Auftrag nicht ausschließlich aus dem Gebiet der EU oder des EWR erbringen, ist nur bei Beachtung der in Kapitel 4 (10) dieses Vertrages genannten Bedingungen möglich. Sie ist insbesondere nur zulässig, soweit und solange der Subunternehmer angemessene Datenschutzgarantien bietet. Der Auftragnehmer teilt dem Auftraggeber mit, welche konkreten Datenschutzgarantien der Subunternehmer bietet und wie ein Nachweis hierüber zu erlangen ist.
- Der Auftragnehmer hat die Einhaltung der Pflichten des Subunternehmers regelmäßig, spätestens alle 12 Monate, angemessen zu überprüfen. Die Prüfung und ihr Ergebnis sind so aussagekräftig zu dokumentieren, dass sie für einen fachkundigen Dritten nachvollziehbar sind. Die Dokumentation ist dem Auftraggeber unaufgefordert vorzulegen. Der Auftragnehmer bewahrt die Dokumentation über durchgeführte Prüfungen mindestens bis zum Ablauf des dritten Kalenderjahres nach Beendigung der Auftragsverarbeitung auf und legt diese dem Auftraggeber auf Verlangen jederzeit vor.
- Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet hierfür der Auftragnehmer gegenüber dem Auftraggeber.
- Zurzeit sind die in Anlage 2 mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt und durch den Auftraggeber genehmigt. Die hier niedergelegten sonstigen Pflichten des Auftragnehmers gegenüber Subunternehmern bleiben unberührt.
- Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservice sind nicht erfasst. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

## 8. Rechte und Pflichten des Auftraggebers

- Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.

**Healthy Codes GmbH**

Am Kartoffelgarten 14,  
81671 München,  
Deutschland

**Geschäftsführer:**

Emad Ahmadi

**Gerichtsstand:** München

HRB 290591

VAT-ID: DE367004887

**Olinda Zweigniederlassung**

Deutschland

DBO 1001 0123 0712 3061

88

QNT0DEB2XXX

- Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.
- Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
- Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind. Der Auftragnehmer ist berechtigt, Kontrollen durch Dritte zu verweigern, soweit diese mit ihm in einem Wettbewerbsverhältnis stehen oder ähnlich gewichtige Gründe vorliegen.
- Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate statt. Soweit der Auftragnehmer den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

## 9. Mitteilungspflichten

- Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes im Auftrag verarbeiteter personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 48 Stunden ab Kenntnis des Auftragnehmers vom relevanten Ereignis an eine vom Auftraggeber benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:
- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

**Healthy Codes GmbH**  
Am Kartoffelgarten 14,  
81671 München,  
Deutschland

**Geschäftsführer:**  
Emad Ahmadi

**Gerichtsstand:** München  
HRB 290591  
VAT-ID: DE367004887

**Olinda Zweigniederlassung**  
Deutschland  
DBO 1001 0123 0712 3061  
88  
QNT0DEB2XXX

- eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen
- Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.
- Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.
- Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 DSGVO im erforderlichen Umfang zu unterstützen.

## 10. Weisungen

- Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.
- Auftraggeber und Auftragnehmer benennen die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen in Anlage 3.
- Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen.
- Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.
- Der Auftragnehmer hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

## 11. Beendigung des Auftrags

- Befinden sich bei Beendigung des Auftragsverhältnisses im Auftrag verarbeitete Daten oder Kopien derselben noch in der Verfügungsgewalt des Auftragnehmers, hat dieser des nach Wahl des Auftraggebers die Daten entweder zu vernichten oder an den Auftraggeber zu übergeben. Die Wahl hat der Auftraggeber innerhalb von 2 Wochen nach entsprechender Aufforderung durch den Auftragnehmer zu treffen. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist.

---

**Healthy Codes GmbH**Am Kartoffelgarten 14,  
81671 München,  
Deutschland**Geschäftsführer:**

Emad Ahmadi

**Gerichtsstand:** München

HRB 290591

VAT-ID: DE367004887

**Olinda Zweigniederlassung**

Deutschland

DBO 1001 0123 0712 3061

88

QNT0DEB2XXX



- Der Auftragnehmer ist verpflichtet, die unverzügliche Vernichtung bzw. Rückgabe auch bei Subunternehmern herbeizuführen.
- Der Auftragnehmer hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Auftraggeber unverzüglich vorzulegen.
- Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer mindestens bis zum Ablauf des dritten Kalenderjahres nach Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber übergeben.

## 12. Vergütung

Die Vergütung des Auftragnehmers ist abschließend im Angebot oder in der Rechnung festgelegt. Eine zusätzliche Vergütung oder Kostenerstattung im Rahmen dieses Vertrages ist ausgeschlossen.

## 13. Haftung

(1) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragnehmer alleine der Auftraggeber gegenüber dem Betroffenen verantwortlich.

(2) Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.

## 14. Sonderkündigungsrecht

- Der Auftraggeber kann diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt und dem Auftragnehmer grobe Fahrlässigkeit oder Vorsatz vorzuwerfen ist, der Auftraggeber eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

**Healthy Codes GmbH**  
Am Kartoffelgarten 14,  
81671 München,  
Deutschland

**Geschäftsführer:**  
Emad Ahmadi

**Gerichtsstand:** München  
HRB 290591  
VAT-ID: DE367004887

**Olinda Zweigniederlassung**  
Deutschland  
DBO 1001 0123 0712 3061  
88  
QNT0DEB2XXX

- Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.
- Bei unerheblichen, insbesondere bei einfachen – also weder vorsätzlichen noch grob fahrlässigen – Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.
- Der Auftragnehmer hat dem Auftraggeber alle Kosten zu erstatten, die diesem durch die verfrühte Beendigung der AGB oder dieses Vertrages in Folge einer außerordentlichen Kündigung durch den Auftraggeber entstehen.

## 15. Sonstiges

- Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.
- Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.
- Für Nebenabreden ist die Schriftform und die ausdrückliche Bezugnahme auf diese Vereinbarung erforderlich.
- Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
- Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

---

**Healthy Codes GmbH**

Am Kartoffelgarten 14,  
81671 München,  
Deutschland

**Geschäftsführer:**

Emad Ahmadi

**Gerichtsstand:** München

HRB 290591

VAT-ID: DE367004887

**Olinda Zweigniederlassung**

Deutschland

DBO 1001 0123 0712 3061

88

QNT0DEB2XXX

## Anlage 1 – technische und organisatorische Maßnahmen

Im Folgenden werden die auftragsbezogenen technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

### 1.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

#### (a) Zutrittskontrolle

##### *Hosting / Datacenter (Pre-live- / Live-Betrieb)*

Angemessene Gewährleistung, da der physische Zugang zu den Rechenzentren auf autorisierte Personen beschränkt ist, um unbefugte Nutzung, Offenlegung, Änderung, Beschädigung oder Verlust von Daten zu verhindern.

##### *Verwaltung & Entwicklung (Dev- / Test)*

- Zugangskontrolle
  - Server sind passwortgeschützt, Zugang besteht nur für berechtigte IT-Mitarbeiter vom Auftragnehmer
  - Zugang zu DV-Geräten mit persönlicher Benutzer-ID und Passwort
  - Passwörter müssen vordefinierter Richtlinie entsprechen
  - Zugang ohne Kennung, Passwort / Private Key nicht möglich
  - Protokollierung der Logins und Passwortfehleingaben

#### (b) Zugriffskontrolle

Gemäß BSI IT-Grundschutz bekommt jeder User nur so viel Berechtigungen erteilt, wie dieser für die Erfüllung seiner Aufgaben benötigt

Zugriff durch personengebundene Accounts

#### (c) Trennungskontrolle

Trennung von Test- und Produktivsystemen

### 1.2 Pseudonymisierung & Verschlüsselung

Grundsätze Privacy-by-Design & Privacy-by-Default werden bereits in der Entwicklungsphase berücksichtigt.

### 1.3 Integrität

#### (a) Weitergabekontrolle

- Alle Mitarbeiter sind i.S.d. Art. 32 Abs.4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen
- Der Zugriff auf die Systeme unterliegt der Zugriffskontrolle
- Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung
- Schutz der Netzwerke gegen Komprimierung durch Firewall
- Nutzung verschlüsselter Netzwerkprotokolle (z.B. HTTPS, SSH)

#### (b) Eingabekontrolle

- Änderungen der Daten werden protokolliert
- Vergabe von Rechten auf Basis eines Berechtigungskonzepts

### 1.4 Verfügbarkeit und Belastbarkeit

#### (a) Verfügbarkeitskontrolle

- Backup- und Recovery-Konzept mit Sicherung aller relevanten Daten

#### (b) Konfigurationsmanagement

- Festplattenspiegelung (RAID) bei allen relevanten Servern
- Monitoring aller relevanter Server, gesonderte Vereinbarungen in der SLA (Live-Betrieb)
- Einsatz unterbrechungsfreier Stromversorgung (USV), Netzersatzanlage im Datacenter
- Zentrales Monitoring und Logging System

#### (c) Belastbarkeit

- Die Umsetzung der Belastbarkeit der bereitgestellten Systeme wird in Absprache mit dem Auftraggeber für das jeweilige Projekt festgelegt
- Die eingesetzten Hosting Partner / Datacenter verfügen über eine ISO-27001 Zertifizierung und entsprechende organisatorische Maßnahmen hinsichtlich Business Continuity Management (BCM) und Disaster Recovery - Art. 32 Abs. 1 lit. c DS-GVO

### 1.5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Benennung eines Datenschutzbeauftragten
- Verpflichtung auf Vertraulichkeit und Aufklärung aller Mitarbeiter
- Grundsatz: Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen bereits in der Konzeptionierung

## Anlage 2 – Zugelassene Subdienstleister

Eine Liste aktuell verwendeter Subdienstleister wird auf der folgenden Seite geführt:

<https://apodienste.de/sub>

## Anlage 3 – Weisungsberechtigte Personen, Adresse zur Meldung von Datenschutzverletzungen

Folgende Personen sind zur Entgegennahme von Weisungen befugt:

Emad Ahmadi Jooghi

[Emad@apodienste.de](mailto:Emad@apodienste.de)

Der Kontakt für Meldungen über die Verletzung personenbezogener Daten erfolgt auf Grundlage der Angaben des Kunden bei der Abgabe seiner Bestellung und basierend auf den von ihm bereitgestellten Kontaktdaten

## Anlage 4 – Datenschutzbeauftragter

Dr. Sebastian Kraska (externer Datenschutzbeauftragter)

IITR Datenschutz GmbH

Marienplatz 2

80331 München

Tel.: +49 (0)89 1891 7360

E-Mail: [email@iitr.de](mailto:email@iitr.de)