**Vereinbarung zur Datenverarbeitung**

zwischen

**«name»**

als für die Verarbeitung Verantwortlicher (im Folgenden "**für die Verarbeitung Verantwortlicher**"),

und

Mediclinic Software Deutschland GmbH, Schönhauser Allee 163, 10435 Berlin

als Datenverarbeiter (im Folgenden "**Datenverarbeiter**",

Der für die Verarbeitung Verantwortliche und der für die Verarbeitung Verantwortliche gemeinsam die "**Parteien**")

**Präambel**

Der für die Verarbeitung Verantwortliche hat den Datenverarbeiter in einem bereits abgeschlossenen Vertrag (nachstehend "**Hauptvertrag**" genannt) für die darin genannten Leistungen beauftragt. Teil der Vertragserfüllung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DSGVO stellt besondere Anforderungen an eine solche Auftragsverarbeitung. Um diesen Anforderungen gerecht zu werden, schließen die Parteien die folgende Datenverarbeitungsvereinbarung (im Folgenden "**Vereinbarung" genannt**), deren Erfüllung nicht gesondert vergütet wird, es sei denn, dies wird ausdrücklich vereinbart.

**§ 1 Begriffsbestimmungen**

(1) Gemäß Art. 4 Abs. 7 DSGVO ist der für die Verarbeitung Verantwortliche die Stelle, die allein oder gemeinsam mit anderen für die Verarbeitung Verantwortlichen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet.

(2) Gemäß Art. 4 Abs. 8 DSGVO ist ein Datenverarbeiter eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

(3) Gemäß Art. 4 Abs. 1 DSGVO sind personenbezogene Daten alle Informationen über eine bestimmte oder bestimmbare natürliche Person (im Folgenden "**betroffene Person**"); als bestimmbar wird eine natürliche Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

(4) Besonders schutzbedürftige personenbezogene Daten sind personenbezogene Daten nach Art. 9 DSGVO, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit der betroffenen Person hervorgehen, personenbezogene Daten gemäß Art. 10 DSGVO über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln, sowie genetische Daten gemäß Art. 4 (13) GDPR, biometrische Daten gemäß Art. 4 (14) GDPR, Gesundheitsdaten gemäß Art. 4 (15) GDPR und Daten über das Sexualleben oder die sexuelle Orientierung einer natürlichen Person.

(5) Nach Artikel 4 Absatz 2 DSGVO ist die Verarbeitung jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, das Ordnen, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Einschränken, Löschen oder Vernichten.

(6) Gemäß Artikel 4 (21) DSGVO ist die Aufsichtsbehörde eine unabhängige staatliche Einrichtung, die von einem Mitgliedstaat gemäß Artikel 51 DSGVO eingerichtet wurde.

**§ 2 Vertragsgegenstand**

(1) Der Datenverarbeiter erbringt die im Hauptvertrag genannten Leistungen für die verantwortliche Stelle. Dabei erhält der Datenverarbeiter Zugang zu personenbezogenen Daten, die er ausschließlich im Auftrag und nach Weisung der verantwortlichen Stelle für diese verarbeitet. Der Umfang und der Zweck der Datenverarbeitung durch den Datenverarbeiter sind im Hauptvertrag und den dazugehörigen Leistungsbeschreibungen festgelegt. Für die Beurteilung der Zulässigkeit der Datenverarbeitung ist der für die Verarbeitung Verantwortliche zuständig.

(2) Die Parteien schließen diese Vereinbarung, um die gegenseitigen datenschutzrechtlichen Rechte und Pflichten festzulegen. Im Zweifelsfall haben die Bestimmungen dieser Vereinbarung Vorrang vor den Bestimmungen des Hauptvertrags.

(3) Die Bestimmungen dieses Vertrages gelten für alle Tätigkeiten im Zusammenhang mit dem Hauptvertrag, bei denen der Datenverarbeiter und seine Mitarbeiter oder von ihm beauftragte Personen mit personenbezogenen Daten in Berührung kommen, die von der verantwortlichen Stelle stammen oder für die verantwortliche Stelle erhoben wurden.

(4) Die Laufzeit dieses Vertrages richtet sich nach der Laufzeit des Hauptvertrages, soweit sich nicht aus den nachfolgenden Bestimmungen weitere Verpflichtungen oder Kündigungsrechte ergeben.

**§ 3 Weisungsrecht**

(1) Der Auftragsverarbeiter darf Daten nur im Rahmen des Hauptvertrags und nach den Weisungen der verantwortlichen Stelle erheben, verarbeiten oder nutzen. Ist der Datenverarbeiter durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu einer Weiterverarbeitung verpflichtet, so hat er die verantwortliche Stelle vor der Verarbeitung über diese rechtlichen Anforderungen zu unterrichten.

(2) Die Weisungen der verantwortlichen Stelle werden zunächst durch diesen Vertrag bestimmt. Danach können sie von der verantwortlichen Stelle in Schrift- oder Textform durch Einzelweisungen (Einzelweisungen) geändert, ergänzt oder ersetzt werden. Die verantwortliche Stelle ist jederzeit berechtigt, solche Weisungen zu erteilen. Dazu gehören auch Weisungen hinsichtlich der Berichtigung, Löschung und Sperrung von Daten.

(3) Alle erteilten Weisungen sind vom Disponenten zu dokumentieren. Weisungen, die über die im Hauptvertrag vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

(4) Ist der Datenverarbeiter der Auffassung, dass eine Weisung der verantwortlichen Stelle gegen datenschutzrechtliche Bestimmungen verstößt, so hat er dies der verantwortlichen Stelle unverzüglich mitzuteilen. Der Auftragsdatenverarbeiter ist berechtigt, die Durchführung der betreffenden Weisung auszusetzen, bis sie von der verantwortlichen Stelle bestätigt oder geändert wird. Der Datenverarbeiter kann sich weigern, eine offensichtlich rechtswidrige Weisung auszuführen.

**§ 4 Arten der verarbeiteten Daten, Gruppe der betroffenen Personen, Drittland**

(1) Der Datenverarbeiter hat im Rahmen der Durchführung des Hauptvertrages Zugriff auf die in **Anlage 1 näher** bezeichneten personenbezogenen Daten.

(2) Der Kreis der von der Datenverarbeitung betroffenen Personen ist in **Anhang 2** aufgeführt.

(3) Eine Übermittlung personenbezogener Daten in ein Drittland darf nur unter den Voraussetzungen der Art. 44 ff. GDPR.

**§ 5 Schutzmaßnahmen des Datenverarbeiters**

(1) Der Datenverarbeiter ist verpflichtet, die gesetzlichen Bestimmungen zum Datenschutz zu beachten und die aus dem Bereich der verantwortlichen Stelle gewonnenen Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind unter Berücksichtigung des Standes der Technik gegen die Kenntnisnahme durch Unbefugte zu sichern.

(2) Der Auftragsverarbeiter hat die interne Organisation in seinem Verantwortungsbereich so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er hat die in **Anlage 3** genannten technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten der verantwortlichen Stelle gemäß Art. 32 DSGVO getroffen, die von der verantwortlichen Stelle als angemessen anerkannt werden. Der Datenverarbeiter behält sich das Recht vor, die getroffenen Sicherheitsmaßnahmen zu ändern und dabei sicherzustellen, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Den bei der Datenverarbeitung durch den Datenverarbeiter beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Datenverarbeiter hat alle von ihm mit der Verarbeitung und Erfüllung dieses Vertrages betrauten Personen (im Folgenden "**Mitarbeiter**") entsprechend zu verpflichten (Verschwiegenheitspflicht, Art. 28 (3) lit. b GDPR) und stellt die Einhaltung dieser Verpflichtung mit der gebotenen Sorgfalt sicher.

(4) Der Auftragsverarbeiter hat einen Datenschutzbeauftragten bestellt. Der Datenschutzbeauftragte des Datenverarbeiters ist die heyData GmbH, Kantstr. 99, 10627 Berlin, datenschutz@heydata.eu, www.heydata.eu.

**§ 6 Informationspflichten des Datenverarbeiters**

(1) Bei Störungen, vermuteten Datenschutzverletzungen oder Verstößen gegen vertragliche Pflichten des Auftragsverarbeiters, vermuteten sicherheitsrelevanten Vorfällen oder sonstigen Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter, durch von ihm im Rahmen des Auftrags eingesetzte Personen oder durch Dritte hat der Auftragsverarbeiter die verantwortliche Stelle unverzüglich zu informieren. Das Gleiche gilt für Überprüfungen des Auftragsverarbeiters durch die Datenschutzaufsichtsbehörde. Die Meldung einer Verletzung des Schutzes personenbezogener Daten muss mindestens die folgenden Angaben enthalten

(a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, einschließlich, soweit möglich, der betroffenen Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;

(b) eine Beschreibung der vom Datenverarbeiter ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung des Verstoßes und gegebenenfalls Maßnahmen zur Abmilderung seiner möglichen nachteiligen Auswirkungen;

(c) eine Beschreibung der voraussichtlichen Folgen der Verletzung des Schutzes personenbezogener Daten.

(2) Der Auftragsverarbeiter trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen, unterrichtet den für die Verarbeitung Verantwortlichen darüber und fordert weitere Anweisungen an.

(3) Darüber hinaus ist der Datenverarbeiter verpflichtet, der verantwortlichen Stelle jederzeit Auskunft zu erteilen, soweit Daten der verantwortlichen Stelle von einer Verletzung nach Absatz 1 betroffen sind.

(4) Der Datenverarbeiter hat die verantwortliche Stelle über wesentliche Änderungen der Sicherheitsmaßnahmen nach § 5 Abs. 2 zu unterrichten.

**§ 7 Kontrollrechte des für die Verarbeitung Verantwortlichen**

(1) Die verantwortliche Stelle kann sich von den technischen und organisatorischen Maßnahmen des Auftragsverarbeiters vor Beginn der Datenverarbeitung und danach regelmäßig in jährlichen Abständen überzeugen. Zu diesem Zweck kann die verantwortliche Stelle z.B. Auskünfte bei dem Auftragsverarbeiter einholen, vorhandene Bescheinigungen von Sachverständigen, Zertifizierungen oder interne Audits einholen oder nach rechtzeitiger Abstimmung die technischen und organisatorischen Maßnahmen des Auftragsverarbeiters während der üblichen Geschäftszeiten persönlich überprüfen oder durch einen fachkundigen Dritten überprüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragsverarbeiter steht. Der für die Verarbeitung Verantwortliche führt die Kontrollen nur in dem erforderlichen Umfang durch und darf dabei den Betrieb des Auftragsverarbeiters nicht unverhältnismäßig stören.

(2) Der Datenverarbeiter verpflichtet sich, der verantwortlichen Stelle auf deren mündliche oder schriftliche Anfrage innerhalb einer angemessenen Frist alle Informationen und Nachweise zur Verfügung zu stellen, die zur Überprüfung der technischen und organisatorischen Maßnahmen des Datenverarbeiters erforderlich sind.

(3) Der für die Verarbeitung Verantwortliche dokumentiert die Ergebnisse der Kontrolle und teilt sie dem Auftragsverarbeiter mit. (4) Stellt die verantwortliche Stelle insbesondere bei der Kontrolle der Ergebnisse der Kontrolle Fehler oder Unregelmäßigkeiten fest, so hat sie den Auftragsverarbeiter unverzüglich zu unterrichten. Werden bei der Kontrolle Tatsachen festgestellt, deren künftige Vermeidung eine Änderung des angeordneten Verfahrens erfordert, so teilt der für die Verarbeitung Verantwortliche dem Auftragsverarbeiter unverzüglich die erforderlichen Verfahrensänderungen mit.

**§ 8 Inanspruchnahme von Dienstleistern**

(1) Die vertraglich vereinbarten Leistungen werden unter Einschaltung der in **Anlage 4** genannten Dienstleister (im Folgenden "**Unterauftragsverarbeiter**") erbracht. Der für die Verarbeitung Verantwortliche erteilt dem Auftragsverarbeiter seine allgemeine Ermächtigung im Sinne von Art. 28 Abs. 2 S. 1 DS-GVO, im Rahmen seiner vertraglichen Verpflichtungen weitere Unterauftragsverarbeiter zu beauftragen oder bereits beauftragte Unterauftragsverarbeiter zu ersetzen.

Option 1:

(2) Der Datenverarbeiter informiert den für die Verarbeitung Verantwortlichen im Voraus per E-Mail-Newsletter über jede beabsichtigte Änderung in Bezug auf die Einschaltung oder den Austausch eines Unterauftragsverarbeiters. Den E-Mail-Newsletter erhält der für die Verarbeitung Verantwortliche, nachdem er eine E-Mail mit dem Betreff "Subscribe" an info@mediclinicsoftware.de gesendet hat. Der für die Verarbeitung Verantwortliche kann der beabsichtigten Beauftragung oder Ersetzung eines Unterauftragsverarbeiters widersprechen, wenn ein wichtiger datenschutzrechtlicher Grund vorliegt.

(3) Der Widerspruch gegen die beabsichtigte Einschaltung oder Ersetzung eines Unterauftragsverarbeiters muss innerhalb von 2 Wochen nach Versendung der Information im E-Mail-Newsletter erfolgen. Erfolgt kein Widerspruch, gilt die Einschaltung oder Ersetzung als genehmigt. Liegt ein wichtiger datenschutzrechtlicher Grund vor und kann keine einvernehmliche Lösung zwischen der verantwortlichen Stelle und dem Auftragsverarbeiter gefunden werden, hat der Auftragsverarbeiter ein Sonderkündigungsrecht zum Ende des auf den Widerspruch folgenden Monats.

Option 2:

(2) Der Datenverarbeiter hat die verantwortliche Stelle vor jeder beabsichtigten Änderung in Bezug auf die Einschaltung oder Ersetzung eines Unterauftragsverarbeiters zu informieren. Der für die Verarbeitung Verantwortliche kann der beabsichtigten Einschaltung oder Ersetzung eines Unterauftragsverarbeiters aus einem wichtigen datenschutzrechtlichen Grund widersprechen.

(3) Der Widerspruch gegen die beabsichtigte Einschaltung oder Ersetzung eines Unterauftragsverarbeiters muss innerhalb von 2 Wochen nach Erhalt der Information über die Änderung erhoben werden. Erfolgt kein Widerspruch, so gilt die Einschaltung oder der Austausch als genehmigt. Liegt ein wichtiger datenschutzrechtlicher Grund vor und ist eine einvernehmliche Lösung zwischen dem Verantwortlichen und dem Auftragsverarbeiter nicht möglich, hat der Verantwortliche ein Sonderkündigungsrecht zum Ende des auf den Widerspruch folgenden Monats.

Ende der Optionen

(4) Bei der Beauftragung von Unterauftragsverarbeitern hat der Datenverarbeiter diese gemäß den Bestimmungen dieser Vereinbarung zu verpflichten.

(5) Ein Unterauftragsverarbeitungsverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragsverarbeiter Dritte mit Dienstleistungen beauftragt, die als reine Hilfsdienste anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versanddienste, Reinigungsdienste, Telekommunikationsdienste ohne besonderen Bezug zu den vom Datenverarbeiter für den Verantwortlichen erbrachten Dienstleistungen und Bewachungsdienste. Wartungs- und Prüfdienste stellen zustimmungspflichtige Unterauftragsverarbeiterverhältnisse dar, soweit sie für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Dienstleistungen für den für die Verarbeitung Verantwortlichen genutzt werden.

**§ 9 Anträge und Rechte der betroffenen Personen**

(1) Der Datenverarbeiter hat die verantwortliche Stelle durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung ihrer Pflichten nach den Artikeln 12-22 und 32 bis 36 DSGVO zu unterstützen.

(2) Macht eine betroffene Person Rechte wie das Recht auf Auskunft, Berichtigung oder Löschung ihrer Daten unmittelbar gegenüber dem Auftragsverarbeiter geltend, so wird dieser nicht selbständig tätig, sondern verweist die betroffene Person an den für die Verarbeitung Verantwortlichen und wartet dessen Weisungen ab.

**§ 10 Haftung**

(1) Im Innenverhältnis zum Auftragsverarbeiter haftet allein die verantwortliche Stelle gegenüber dem Betroffenen auf Ersatz des Schadens, der dem Betroffenen durch eine unzulässige oder unrichtige datenschutzrechtliche Verarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung entsteht.

(2) Der Datenverarbeiter haftet unbeschränkt für Schäden, soweit die Schadensursache auf einer vorsätzlichen oder grob fahrlässigen Pflichtverletzung des Datenverarbeiters, seines gesetzlichen Vertreters oder Erfüllungsgehilfen beruht.

(3) Der Auftragsverarbeiter haftet für fahrlässiges Verhalten nur bei der Verletzung einer Pflicht, deren Erfüllung die ordnungsgemäße Durchführung des Vertrages überhaupt erst ermöglicht und auf deren Einhaltung die verantwortliche Stelle regelmäßig vertraut und vertrauen darf, jedoch begrenzt auf den vertragstypischen Durchschnittsschaden. Im Übrigen ist die Haftung des Auftragsverarbeiters - auch für seine Erfüllungsgehilfen - ausgeschlossen.

(4) Die Haftungsbeschränkung nach § 10.3 gilt nicht für Schadensersatzansprüche aus der Verletzung des Lebens, des Körpers, der Gesundheit oder aus der Übernahme einer Garantie.

**§ 11 Beendigung des Hauptvertrages**

(1) Nach Beendigung des Hauptvertrages hat der Auftragsverarbeiter alle ihm überlassenen Unterlagen, Daten und Datenträger an die verantwortliche Stelle zurückzugeben oder - auf Verlangen der verantwortlichen Stelle, soweit nicht nach Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Pflicht zur Aufbewahrung der personenbezogenen Daten besteht - zu löschen. Dies gilt auch für etwaige Datensicherungen beim Auftragsverarbeiter. Der Auftragsverarbeiter hat auf Verlangen einen Nachweis über die ordnungsgemäße Löschung der Daten zu erbringen.

(2) Die verantwortliche Stelle hat das Recht, die vollständige und vertragsgemäße Rückgabe oder Löschung der Daten beim Datenverarbeiter in geeigneter Weise zu kontrollieren.

(3) Der Auftragsverarbeiter ist verpflichtet, die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten auch über das Ende des Hauptvertrages hinaus geheim zu halten. Diese Vereinbarung gilt über das Ende des Hauptvertrages hinaus, solange der Auftragsverarbeiter über personenbezogene Daten verfügt, die ihm von der verantwortlichen Stelle übermittelt wurden oder die er für die verantwortliche Stelle erhoben hat.

**§ 12 Schlussbestimmungen**

(1) Soweit der Auftragsverarbeiter Unterstützungsleistungen im Rahmen dieses Vertrages nicht ausdrücklich unentgeltlich erbringt, kann er der verantwortlichen Stelle hierfür ein angemessenes Entgelt in Rechnung stellen, es sei denn, eigene Handlungen oder Unterlassungen des Auftragsverarbeiters haben eine solche Unterstützung unmittelbar erforderlich gemacht.

(2) Änderungen und Ergänzungen dieses Vertrages bedürfen der Schriftform. Dies gilt auch für einen Verzicht auf dieses Formerfordernis. Der Vorrang einzelvertraglicher Vereinbarungen bleibt hiervon unberührt.

(3) Sollten einzelne Bestimmungen dieses Vertrages ganz oder teilweise unwirksam oder undurchführbar sein oder werden, so wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt.

(4) Diese Vereinbarung unterliegt dem deutschen Recht.

**Controller**

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Position: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Datum: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Unterschrift: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Datenverarbeiter**

Name: Marcus Doille

Position: Geschäftsführender Direktor

Datum: 1. März 2023

Unterschrift:

**Anhang**

**Anhang 1 - Beschreibung der Daten/Datenkategorien**

* Vor- und Nachname
* E-Mail-Adressen
* Adressen
* Telefonnummern
* Krankenversicherungsnummer
* Gesundheitsdaten (z. B. Diagnosen, Untersuchungsergebnisse, Bescheinigungen usw.)
* Andere personenbezogene Daten, die von den Nutzern des Produkts in der Cloud gespeichert werden

**Anhang 2 - Beschreibung der betroffenen Personen/Gruppen von betroffenen Personen**

* Patienten
* Ärzte
* Personal der medizinischen Klinik

**Anhang 3 - Technische und organisatorische Maßnahmen des Datenverarbeiters**

**1. Einleitung**

Dieses Dokument fasst die technischen und organisatorischen Maßnahmen des Auftragsverarbeiters im Sinne von Artikel 32 (1) DSGVO zusammen. Dies sind Maßnahmen, mit denen der Auftragsverarbeiter personenbezogene Daten schützt.

**2. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)**

**2.1. Physische Zugangskontrolle**

Die folgenden Maßnahmen verhindern, dass sich Unbefugte Zugang zu den Datenverarbeitungsanlagen verschaffen können:

* Manuelles Schließsystem (z. B. Schlüssel)
* Sicherheitsschlösser
* Klingelanlage mit Kamera
* Besucher nur in Begleitung von Mitarbeitern
* Anweisung an die Mitarbeiter, nicht in öffentlich zugänglichen Räumen (z. B. Cafés) zu arbeiten
* Arbeit im häuslichen Arbeitszimmer: Weisen Sie Ihre Mitarbeiter an, wenn möglich, in einem vom Wohnbereich getrennten Arbeitszimmer zu arbeiten.

**2.2. Logische Zugangskontrolle**

Die folgenden Maßnahmen verhindern den Zugriff Unbefugter auf die Datenverarbeitungssysteme:

* Authentifizierung mit biometrischen Daten
* Verwendung von Antiviren-Software
* Einsatz einer Firewall
* Einsatz von Mobile Device Management
* Verschlüsselung von Datenträgern
* Smartphone-Verschlüsselung
* Verschlüsselung von Notebooks/Tablets
* Verwaltung von Benutzerberechtigungen
* Benutzerprofile erstellen
* Zentrale Passwortregeln
* Verwendung der 2-Faktor-Authentifizierung

**2.3 Berechtigungskontrolle**

Die folgenden Maßnahmen stellen sicher, dass Unbefugte keinen Zugang zu personenbezogenen Daten haben:

* Einsatz von Aktenvernichtern (mit Cross-Cut-Funktion)
* Verwendung eines Berechtigungskonzepts
* Die Anzahl der Administratoren wird so gering wie möglich gehalten.
* Sichere Aufbewahrung von Datenträgern
* Verwaltung von Benutzerrechten durch Systemadministratoren

**2.4 Trennungskontrolle**

Die folgenden Maßnahmen stellen sicher, dass personenbezogene Daten, die für unterschiedliche Zwecke erhoben wurden, getrennt verarbeitet werden:

* Trennung von Produktiv- und Testsystem
* Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
* Versehen der Datensätze mit Zweckattributen/Datenfeldern

**3. Integrität (Art. 32 Abs. 1 lit. b DSGVO)**

**3.1 Kontrolle der Übermittlung**

Es wird sichergestellt, dass personenbezogene Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft werden kann, welche Personen oder Stellen personenbezogene Daten erhalten haben. Um dies zu gewährleisten, werden die folgenden Maßnahmen durchgeführt:

* E-Mail-Verschlüsselung
* Bereitstellung von Daten über verschlüsselte Verbindungen wie SFTP oder HTTPS

**3.2 Eingabekontrolle**

Die folgenden Maßnahmen gewährleisten, dass überprüft werden kann, wer zu welchem Zeitpunkt personenbezogene Daten in Datenverarbeitungssystemen verarbeitet hat:

* Manuelle oder automatische Kontrolle der Protokolle
* Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf der Grundlage eines Berechtigungskonzepts

**4. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)**

Die folgenden Maßnahmen stellen sicher, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und dem Kunden jederzeit zur Verfügung stehen:

* Sicherung der Daten an einem sicheren, externen Ort
* Trennung von Betriebssystemen und Daten
* Hosting (zumindest der wichtigsten Daten) bei einem professionellen Hoster

**5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32(1)(d) GDPR; Art. 25(1) GDPR)**

**5.1 Verwaltung des Datenschutzes**

Die folgenden Maßnahmen sollen sicherstellen, dass eine Organisation vorhanden ist, die die grundlegenden Anforderungen des Datenschutzrechts erfüllt:

* Nutzung der heyData-Plattform für die Verwaltung der Datensicherung
* Ernennung des Datenschutzbeauftragten heyData
* Verpflichtung der Mitarbeiter auf das Datengeheimnis
* Regelmäßige Schulungen der Mitarbeiter zum Thema Datenschutz
* Überblick über die Verarbeitungstätigkeiten (Art. 30 GDPR)

**5.2 Management der Reaktion auf Vorfälle**

Die folgenden Maßnahmen sollen sicherstellen, dass bei Datenschutzverletzungen Meldeverfahren eingeleitet werden:

* Verfahren zur Meldung von Datenschutzverletzungen gemäß Art. 4 Nr. 12 GDPR an die Aufsichtsbehörden (Art. 33 GDPR)
* Verfahren zur Benachrichtigung bei Datenschutzverletzungen gemäß Art. 4 Nr. 12 DSGVO gegenüber den betroffenen Personen (Art. 34 DSGVO)
* Einschaltung des Datenschutzbeauftragten bei Sicherheitsvorfällen und Datenschutzverletzungen
* Verwendung von Antiviren-Software
* Einsatz einer Firewall

**5.3 Datenschutzfreundliche Voreinstellungen (Art. 25 (2) GDPR)**

Die folgenden Maßnahmen tragen den Anforderungen der Grundsätze "Privacy by Design" und "Privacy by Default" Rechnung:

* Schulung der Mitarbeiter in "Privacy by design" und "Privacy by default".
* Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.

**5.4 Auftragskontrolle**

Die folgenden Maßnahmen stellen sicher, dass personenbezogene Daten nur gemäß den Anweisungen verarbeitet werden können:

* Schriftliche Weisungen an den Auftragnehmer oder Weisungen in Textform (z.B. durch Auftragsbearbeitungsvertrag)
* Sicherstellung der Vernichtung der Daten nach Abschluss des Auftrags, z. B. durch Einholung entsprechender Bestätigungen
* Bestätigung der Auftragnehmer, dass sie ihre eigenen Mitarbeiter auf das Datengeheimnis verpflichten (in der Regel im Auftragsverarbeitungsvertrag)
* Sorgfältige Auswahl von Auftragnehmern (insbesondere im Hinblick auf die Datensicherheit)
* Laufende Überprüfung der Auftragnehmer und ihrer Tätigkeiten

**Anhang 4 - Derzeitige Unterauftragsverarbeiter**

|  |  |  |
| --- | --- | --- |
| **Name** | **Funktion** | **Standort des Servers** |
| Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA | Hosting | EU (Frankfurt) |
| BlueSnap Corporate, 800 South St., Suite 640, Waltham, MA, USA | Zahlungsanbieter | USA |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |