



# Vertraulichkeitsvereinbarung

zwischen

helpwave GmbH  
c/o Collective Incubator, 3. OG  
Jülicher Straße 209d  
52070 Aachen  
NRW Deutschland  
Aachen HRB 27480  
(nachfolgend „Inhaber“)

und

(nachfolgend „Empfänger“)

(nachfolgend beide Parteien auch bezeichnet als „Partei“ oder „Parteien“)

## Präambel

Die Parteien beabsichtigen die Durchführung eines gemeinsamen Projekts im Zusammenhang mit

Der Entwicklung und Ausführung von Digitalisierungslösungen im Gesundheitsbereich durch die dafür gegründete helpwave GmbH und/oder ihrer Töchtergesellschaften und/oder mit ihr verbundener Unternehmen/Gesellschaften. (nachfolgend „Zweck“).

Der Inhaber beabsichtigt, für den vorstehend beschriebenen Zweck dem Empfänger vertrauliche Informationen gemäß nachstehender Ziffer 1 zur Verfügung zu stellen. Dem Empfänger ist bewusst, dass diese vertraulichen Informationen bisher weder insgesamt noch in ihren Einzelheiten bekannt oder ohne weiteres zugänglich waren, deshalb von wirtschaftlichem Wert sind und seitens des Inhabers durch angemessene Geheimhaltungsmaßnahmen geschützt sind.

Sofern eine vertrauliche Information nach dieser Vertraulichkeitsvereinbarung (nachfolgend „Vereinbarung“) nicht den Anforderungen eines Geschäftsgeheimnisses im Sinne des Geschäftsgeheimnisgesetzes genügt, unterfällt diese Information dennoch den Vertraulichkeitsverpflichtungen nach dieser Vereinbarung.

# 1 Vertrauliche Informationen

**1.1** Vertrauliche Informationen im Sinne dieser Vereinbarung sind sämtliche Informationen (ob schriftlich, elektronisch, mündlich, digital verkörpert oder in anderer Form), die von dem Inhaber direkt oder indirekt an den Empfänger oder einem mit Empfänger im Sinne der §§ 15 ff. AktG verbundenen Unternehmen zum vorgenannten Zweck seit Aufnahme der Tätigkeit offenbart werden bzw. worden sind. Als vertrauliche Informationen gelten insbesondere:

**1.1.1** Geschäftsgeheimnisse, Produkte, Herstellungsprozesse, Know-how, Erfindungen, geschäftliche Beziehungen, Geschäftsstrategien, Businesspläne, Finanzplanung, Personalangelegenheiten, die beauftragten Leistungen und sonstige Arbeitsergebnisse;

**1.1.2** Jegliche Unterlagen und Informationen des Inhabers, die Gegenstand technischer und organisatorischer Geheimhaltungsmaßnahmen sind und als vertraulich gekennzeichnet oder nach der Art der Information oder den Umständen der Übermittlung als vertraulich anzusehen sind;

**1.1.3** Informationen, die nach Ziff. 1 als vertrauliche Informationen gelten und die der Empfänger bereits vor Unterzeichnung dieser Vereinbarung im Rahmen des Zwecks erhalten hat;

**1.1.4** der Inhalt dieser Vereinbarung.

**1.2** Keine vertrauliche Informationen sind solche Informationen,

**1.2.1** die der Öffentlichkeit vor der Mitteilung oder Übergabe durch den Inhaber bekannt oder allgemein zugänglich waren oder dies zu einem späteren Zeitpunkt ohne Verstoß gegen eine Geheimhaltungspflicht werden;

**1.2.2** die dem Empfänger bereits vor der Offenlegung durch den Inhaber und ohne Verstoß gegen eine Geheimhaltungspflicht nachweislich bekannt waren;

**1.2.3** die von dem Empfänger ohne Nutzung oder Bezugnahme auf vertrauliche Informationen von dem Inhaber selber gewonnen wurden; oder

**1.2.4** die der Empfänger von einem berechtigten Dritten ohne Verstoß gegen eine Geheimhaltungspflicht übergeben oder zugänglich gemacht werden.

## 2 Geheimhaltungspflichten

Der Empfänger verpflichtet sich,

**2.1** die vertraulichen Informationen streng vertraulich zu behandeln und nur im Zusammenhang mit dem Zweck zu verwenden;

**2.2** die vertraulichen Informationen nur gegenüber solchen Vertretern offen zu legen, die auf die Kenntnis dieser Informationen für den Zweck angewiesen sind, vorausgesetzt, dass der Empfänger sicherstellt, dass ihre Vertreter diese Vereinbarung einhalten, als wären sie selbst durch diese Vereinbarung gebunden;

**2.3** die vertraulichen Informationen ebenfalls durch angemessene Geheimhaltungsmaßnahmen gegen den unbefugten Zugriff durch Dritte zu sichern und bei der Verarbeitung der vertraulichen Informationen die gesetzlichen und vertraglichen Vorschriften zum Datenschutz einzuhalten. Dies beinhaltet auch dem aktuellen Stand der Technik angepasste technische Sicherheitsmaßnahmen (Art. 32 DS-GVO) und die Verpflichtung der Mitarbeiter auf die Vertraulichkeit und die Beachtung des Datenschutzes (Art. 28 Abs. 3 lit. b DS-GVO) sowie weitere in dieser Vereinbarung oder sonstige zwischen den Parteien diesbezüglich getroffene vertragliche Vereinbarungen;

**2.4** sofern der Empfänger aufgrund geltender Rechtsvorschriften gerichtlicher oder behördlicher Anordnungen oder aufgrund einschlägiger börsenrechtlicher Regelungen verpflichtet ist, teilweise oder sämtliche Vertraulichen Informationen offenzulegen, den Inhaber (soweit rechtlich möglich und praktisch umsetzbar) hierüber unverzüglich schriftlich zu informieren und alle zumutbaren Anstrengungen zu unternehmen, um den Umfang der Offenlegung auf ein Minimum zu beschränken und dem Inhaber erforderlichenfalls jede zumutbare Unterstützung zukommen zu lassen, die eine Schutzanordnung gegen die Offenlegung sämtlicher Vertraulicher Informationen oder von Teilen hiervon anstrebt.

### **3 Sicherheitsvereinbarung**

Der Empfänger kann zur Durchführung des Projekts bzw. Erfüllung des Zweckes Zugang zur technischen Administration der IT - Systeme des Inhabers und gegebenenfalls den Kommunikationsmitteln des Inhabers erhalten.

**3.1** Zur Erfüllung der Anforderungen des Datenschutzes und der informationstechnischen Sicherheit verpflichtet sich der Empfänger unbeschadet der in Ziff. 2 genannten Pflichten zur Einhaltung der folgenden Sicherheitsmaßnahmen:

**3.1.1** Ausschließliche Nutzung der durch den Inhaber gestellten VPN-Verbindung für den Zweck von Arbeiten an Kundendaten (z.B. Backups, Wartungen);

**3.1.2** Nutzung von Informationen und Daten ausschließlich zur Erfüllung der vereinbarten Aufgaben;

**3.1.3** Ausschließliche Verwendung von Systemen, welche ausgiebig nach besten Wissen durch den Empfänger überprüft wurden;

**3.1.4** Nutzung nur der im Rahmen der vereinbarten Leistung zugewiesenen Rechte;

**3.1.5** Sofortige Meldung von erkannten Sicherheitslücken an den Inhaber.

**3.2** Die Vereinbarung von den in 3.1 genannten abweichenden Sicherheitsmaßnahmen muss schriftlich erfolgen. Die einfache elektronische Signatur ist ausreichend.

## **4 Rückgabe bzw. Löschung der vertraulichen Informationen**

**4.1** Auf Aufforderung des Inhabers oder bei Beendigung der Zusammenarbeit ist der Empfänger verpflichtet, sämtliche bzw. in dem Inhaber bestimmtem Umfang vertrauliche Informationen einschließlich der Kopien hiervon innerhalb von zehn (10) Arbeitstagen nach Zugang der Aufforderung bzw. nach Beendigung der Zusammenarbeit zurückzugeben oder zu vernichten (einschließlich elektronisch gespeicherter vertraulicher Informationen), sofern nicht mit dem Inhaber vereinbarte oder gesetzliche Aufbewahrungspflichten dem entgegenstehen.

**4.2** Die Vernichtung elektronisch gespeicherter vertraulicher Informationen erfolgt durch die vollständige und unwiderrufliche Löschung der Dateien oder unwiederbringliche Zerstörung des Datenträgers. Vollständige und unwiderrufliche Löschung bedeutet bei elektronisch gespeicherten vertraulichen Informationen, dass die vertraulichen Informationen derart gelöscht werden, dass jeglicher Zugriff auf diese Informationen unmöglich wird, wobei ein Lösungsverfahren verwendet wird, welche den anerkannten Standards genügen. Nach Löschung dieser Informationen dürfen keine Wiederherstellungsverfahren oder Verfahren die zur Wiederlesbarkeit der Informationen führen können, angewandt oder für Dritte ermöglicht werden.

**4.3** Ausgenommen hiervon sind – neben vertraulichen Informationen, bzgl. derer eine Aufbewahrungspflicht i.S.d. Ziffer 4.1 besteht – vertrauliche Informationen, deren Vernichtung bzw. Rückgabe technisch nicht möglich ist, z.B. da sie aufgrund eines automatisierten elektronischen Backup-Systems zur Sicherung von elektronischen Daten in einer Sicherungsdatei gespeichert wurden; hierzu zählt auch das technisch notwendige Vorhalten von Stammdaten (z.B. Personal- oder Kundennummern), welches nötig ist, um eine Verknüpfung zu den archivierten Informationen herzustellen.

**4.4** Auf Verlangen des Inhabers hat der Empfänger schriftlich zu versichern, dass er sämtliche vertrauliche Informationen nach den Maßgaben der vorstehenden Ziffern und den Weisungen des Inhabers vollständig und unwiderruflich gelöscht hat.

## **5 Eigentumsrechte an den vertraulichen Informationen**

**5.1** Der Inhaber hat, unbeschadet der Rechte, die er nach dem GeschGehG hat, hinsichtlich der vertraulichen Informationen alle Eigentums-, Nutzungs- und Verwertungsrechte. Der Inhaber behält sich das ausschließliche Recht zur Schutzrechtsanmeldung vor. Der Empfänger erwirbt kein Eigentum oder – mit Ausnahme der Nutzung für den oben beschriebenen Zweck – sonstige Nutzungsrechte an den vertraulichen Informationen (insbesondere an Know-how, darauf angemeldeten oder erteilten Patenten, Urheberrechten oder sonstigen Schutzrechten) aufgrund dieser Vereinbarung oder sonst wegen konkludenten Verhaltens.

**5.2** Der Empfänger hat es zu unterlassen, die vertraulichen Informationen außerhalb des Zwecks in irgendeiner Weise selbst wirtschaftlich zu verwerten oder nachzuahmen (insbesondere im Wege des sog. „Reverse Engineering“) oder durch Dritte verwerten oder nachahmen zu lassen und insbesondere auf die vertraulichen Informationen gewerbliche Schutzrechte – insbesondere Marken, Designs, Patente oder Gebrauchsmuster – anzumelden.

## 6 Vertragsstrafe

Verletzt der Empfänger oder Mitarbeiter des Empfängers oder sonstige Personen, für die der Empfänger gemäß §§ 31, 278, 831 BGB einzustehen hat, die sich aus dieser Vereinbarung ergebenden Pflichten, so vereinbaren die Parteien die Zahlung einer verschuldensunabhängigen Vertragsstrafe durch den Empfänger an den Inhaber in angemessener Höhe, wobei der Inhaber die Höhe nach billigem Ermessen i.S.v. § 315 BGB bestimmen wird und die Angemessenheit der Vertragsstrafe im Streitfall von dem zuständigen Gericht überprüft werden kann.

Die Geltendmachung weiteren Schadensersatzes bleibt vorbehalten.

## 7 Laufzeit

Diese Vereinbarung tritt nach Unterzeichnung in Kraft und endet zwei Jahre nach Beendigung des Informationsaustausches zum vorgenannten Zweck oder der Zusammenarbeit der Parteien. Die Pflicht zur Geheimhaltung bleibt von der Beendigung dieser Vereinbarung unberührt.

## 8 Anwendbares Recht und Gerichtsstand

Die Bestimmungen dieser Vereinbarung unterliegen in ihrer Durchführung und Auslegung deutschem Recht unter Ausschluss des internationalen Privatrechts. Ausschließlicher Gerichtsstand für Streitigkeiten aus oder im Zusammenhang mit der Vereinbarung ist Aachen, Deutschland.

## 9 Schlussbestimmungen

**9.1** Die vorliegende Vereinbarung stellt die gesamte zwischen den Parteien getroffene Vereinbarung dar und ersetzt alle früheren Vereinbarungen zum oben genannten Zweck. Mündliche Nebenabreden bestehen nicht. Änderungen und Ergänzungen dieser Vereinbarung sowie Kündigungen bedürfen der Schriftform, wobei – sofern nicht anderweitig in dieser Vereinbarung bestimmt – die einfache elektronische Signatur ausreicht. Dies gilt auch für eine Änderung bzw. Aufhebung dieser Klausel.

**9.2** Sollten eine oder mehrere Bestimmungen dieses Vertrags rechtsunwirksam sein oder werden, so soll dadurch die Gültigkeit der übrigen Bestimmungen nicht berührt werden. Die Parteien verpflichten sich, die unwirksame Bestimmung durch eine Regelung zu ersetzen, die dem mit ihr angestrebten wirtschaftlichen Zweck am nächsten kommt.

---

Inhaber

---

## Empfänger

### Anlage

#### Projektbeschreibung und Vertrauliche Informationen vom 20. Dezember 2024

Die helpwave GmbH entwickelt digitale Lösungen im Gesundheitsbereich und bietet diese im B2B, ggf. auch im B2C Bereich entgeltlich an. Insbesondere entwickelt sie Lösungen für das Informationsmanagement im ambulanten und stationären Bereich, ggf. unter Hinzunahme von auf Machine Learning und/oder künstlicher Intelligenz basierenden Algorithmen. Dafür entwickelt sie Nutzeroberflächen für die EndnutzerInnen, ebenso wie diese zugrunde liegende Softwareinfrastruktur und hält die für die Benutzung der Programme/Systeme notwendige Infrastruktur (Software/Hardware) direkt oder indirekt vor. Als Beispiele für vertrauliche Informationen in diesem Kontext gelten u.a die System- und Serverarchitektur (falls nicht durch ein Open-Source Repository anders vorgesehen), Kundendaten inkl. der iRd Nutzung oder bei der Analyse derselben anfallende Daten (auch soweit sie nicht als personenbezogene Daten unter das Datenschutzrecht fallen) und jegliche auf helpwave bezogene Informationen, insb. auch Kommunikationsdaten und -inhalte und Dateien. Als Unternehmen, welches sich den Prinzipien des Open Source Ansatzes verpflichtet sieht, stellt helpwave so viele Informationen wie möglich interessierten Dritten zur Verfügung. Im Umkehrschluss sind nicht veröffentlichte Informationen zunächst einmal auch ohne gesonderte Kennzeichnung als vertraulich zu betrachten (s. Ziff. 1.1.2)