Technische und organisatorische Maßnahmen (TOM)

i.S.d. Art. 32 DSGVO

helpwave GmbH
c/o Collective Incubator
Jülicher Straße 209q-s
52070 Aachen
NRW Deutschland
Aachen HRB 27480

22. Januar 2026

Inhaltsverzeichnis

1 Übersicht

Das folgende Dokument beschreibt die technischen und organisatorischen Maßnahmen (TOM) i.S.v. Art. 32 DSGVO, die wir als Unternehmen ergreifen, um die Rechte und Freiheiten natürlicher Personen im Bereich des Datenschutzes zu schützen. Unser Ziel ist es, mit unseren Lösungen die Gesundheitsversorgung durch digitale Anwendungen zu unterstützen. Die hier beschriebenen Maßnahmen ergreifen wir unternehmensweit, d.h. sie gelten grundsätzlich für all unsere Produkte und Lösungen. Aufgrund der in Einzelfällen anhand der Bedürfnisse der KundenInnen orientierten spezifischen Umsetzung unserer Lösungen kann es jedoch in Absprache mit den KundInnen zu Abweichungen kommen. Darüber hinaus sind für die einzelnen Produkte, wie beispielsweise helpwave tasks, die für den Datenschutz relevanten Besonderheiten in einem separaten Dokument aufgeführt.

1.1 Grundprinzipien Die Grundprinzipen unseren Datenschutzkonzepts sind separat aufgeführt. Die Verarbeitung personenbezogener Daten richtet sich insbesondere nach Art. 5 DS-GVO sowie in Bezug auf besondere Kategorien personenbezogener Daten wie Gesundheitsdaten nach Art. 9 DS-GVO bzw. § 22 BDSG. Für Einzelheiten und Besonderheiten mit Blick auf unsere unterschiedlichen Produkte und Dienstleistungen verweisen wir, sofern gegeben, auf die produkteigene Dokumentation zum Thema Datenschutz. Wesentlich für die von uns getroffenen technischen und organisatorischen Maßnahmen ist die grundlegende Unterscheidung zwischen Daten, die im Vertragsverhältnis zwischen uns und unseren KundInnen und den Daten, die durch die Nutzung unserer Produkte verarbeitet werden. Letztere können damit neben personenbezogenen Daten der NutzerInnen auch personenbezogene Daten Dritter sein. Diese Unterscheidung vollziehen wir durch ein strenges Berechtigungsmanagement (s.u. Rollenkonzeption) und den Grundsatz der Datensparsamkeit nach. Darüber hinaus ist Datenschutz dynamisch - wir re-evaluieren unsere Maßnahmen regelmäßig und passen sie an die jeweils aktuellen Bedürfnisse und Möglichkeiten an.

1.2 Definitionen

- Anwendungen: Digitale Produkte der helpwave GmbH, die entweder webbasiert oder auf mobilen Endgeräten als Programm (Applikation) genutzt werden.
- Anwendungsdaten: Daten, die durch die konkrete Nutzung der Anwendungen generiert werden; das kann sowohl Daten von NutzerInnen wie auch Dritten umfassen.
- Kundenstammdaten: Daten, die im Kontext der Vertragsanbahnung und -durchführung verarbeitet werden, jedoch keine Anwendungsdaten sind.
- Kritische Dienste: IT-Dienste oder Komponenten, deren Ausfall oder Kompromittierung wesentliche Auswirkungen auf die Sicherheit, Integrität oder Verfügbarkeit der Anwendungen oder der Datenverarbeitung hat.
- Datenhaltende Systeme, datenhaltende Server: IT-Systeme oder Server, auf denen Anwendungsdaten, Kundendaten oder andere geschäftskritische Informationen gespeichert, verarbeitet oder übermittelt werden.
- Sicherheitsverletzungen: Unbefugter Zugriff auf Daten, deren Verlust, Veränderung oder Veröffentlichung sowie jede andere Form der Beeinträchtigung von Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen oder Systemen.
- Sicherheitsvorfall: Ein einzelnes Ereignis oder eine Kette zusammenhängender Ereignisse mit Bezug zur Informationssicherheit, das bzw. die eine Sicherheitsverletzung zur Folge haben kann oder

bereits hatte.

1.3 Anwendungen Die helpwave GmbH bietet aktuell unterschiedliche Anwendungen bzw. Produkte an.

- helpwave tasks (lokal)
- mediQuu Netzmanager (cloud)
- App zum Doc (cloud)
- mediQuu viva (hybrid)

1.4 Kontext der Datenverarbeitung Im Sinne der nachfolgend dargestellten technisch-organisatorischen Maßnahmen lassen sich unterschiedliche Datenverarbeitunszusammenhänge unterscheiden: Kundenstammdaten werden im Kontext der Vertragsanbahung und -erfüllung verarbeitet. Dazu gehören beispielsweise Stammdaten der Kunden oder abrechnungsrelevante Daten. Davon abzugrenzen sind Daten, die im Rahmen der Nutzung unserer Produkte verarbeitet werden. Hier lassen sich wieder Daten der NutzerInnen von Daten Dritter unterscheiden. Bei der Nutzung der Anwendungen können sowohl allgemeine Angaben über die NutzerInnen (z.B. Profilangaben zur Authentifizierung oder Angaben zur Funktion innerhalb der Organisation, die die Anwendung nutzt), als auch Daten Dritter, beispielsweise PatientInnen, verarbeitet werden.
Soweit und sofern die helpwave GmbH in den jeweiligen Zusammenhängen nicht als Verantwortliche sondern als Auftragsverarbeiterin auftritt, liegt es in der Verantwortlichkeit des Kunden, die für die rechtmäßige Verarbeitung personenbezogener Daten notwendige Einwilligung einzuholen, sofern kein gesetzlicher Tatbestand jene ermöglicht.

1.5 Räumlichkeiten Die Räumlichkeiten, in denen es zu einer Datenverarbeitung kommen kann, hängen einerseits vom Kontext der Datenverarbeitung (s.o.), andererseits von der konkret eingesetzten Anwendung ab. Es werden unterschieden:

- Büroräume der helpwave GmbH.
- Rechenzentren, die durch Unterauftragnehmer zur Verfügung gestellt werden. helpwave nutzt für den Betrieb der datenhaltenden Server die Hetzner Online GmbH (im Folgenden „Hetzner“), die Unterauftragnehmerin von helpwave ist.

Die helpwave GmbH strebt an, die Anwendungen lokal auf den Servern der KundInnen zu installieren und operieren zu lassen. Ist dies der Fall, ist der/die jeweilige KundIn für die Maßnahmen zur Sicherung der Vertraulichkeit und Integrität, insbesondere der Zugangsbeschränkung, verantwortlich.
Nachfolgende Ausführungen zum Bereich „Rechenzentren“ beziehen sich immer auf die Rechenzentren der Hetzner Online GmbH. Die Unterauftragnehmer sind vertraglich gebunden und werden entsprechend der Vereinbarung zur Auftragsvereinbarung durch helpwave geprüft.
Im Folgenden wird daher – sofern erforderlich bzw. zielführend – zwischen Maßnahmen für die Rechenzentren und für die Büroräume von helpwave unterschieden.
Weitere Informationen zu den Technisch-organisatorischen Maßnahmen der Rechenzentrumsbetreiber finden Sie hier:

- Hetzner: www.hetzner.com

1.6 Mobiles Arbeiten Die helpwave GmbHermöglicht allen ihren Mitarbeitenden außerhalb der o.g. Räumlichkeiten zu arbeiten und dazu erlaubt dazu den Einsatz von Laptops und Smartphones. Sofern und soweit Mitarbeitende der helpwave GmbHdieses Angebot wahrnehmen, sind sie verpflichtet, die in diesem Dokument aufgezeigten technisch-organisatorischen Maßnahmen einzuhalten.

1.7 Rollenkonzeption Um sicherzustellen, dass der Zugriff auf und die Verarbeitung von Daten nur durch Personen erfolgt, deren Tätigkeit innerhalb der helpwave GmbHdies tatsächlich erfordert, existiert ein differenziertes Stufenkonzept, welches unterschiedliche Funktionen in Hinblick auf datenschutzrelevante Tätigkeiten definiert. Diesen unterschiedlichen Funktionen sind jeweilige Berechtigungen zugewiesen. Daran anknüpfend existieren differenzierte Anforderungen an beispielsweise Maßnahmen zu Zugangskontrolle.

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

2.1 Zutrittskontrolle

2.1.1 Rechenzentrum Die Rechenzentren der von helpwave beauftragten Unterauftragnehmer erfüllen mindestens folgende Anforderungen an:

- Alarmüberwachung
- Personenüberprüfung und -identifikation bei Zutritt
- Zutrittsprotokollierung
- Kameraüberwachung sowie Bewegungs- und Einbruchsmelder
- Personenkontrolle und -überwachung durch Vor-Ort-Personal

Diese Sicherheitsmaßnahmen werden durch die Unterauftragnehmer rund um die Uhr an sieben Tagen pro Woche sichergestellt.

2.1.2 Büroräume Die Büroräume der helpwave GmbH liegen in der helpwave GmbH
c/o Collective Incubator
Jülicher Straße 209q-s
52070Aachen
Nordrhein-Westfalen
Deutschland. In diesen Büroräumen befinden sich keine stationären Datenverarbeitungsanlagen, die zur Verarbeitung von Daten der Kunden von helpwave genutzt werden. Die Verarbeitung von Daten erfolgt ausschließlich auf mobilen Geräten, die nach Maßgabe dieser technisch-organisatorischen Maßnahmen gesichert sind und nur durch autorisierte Personen.
Der Zugang zu den Büroräumen ist durch folgende Maßnahmen geschützt:

- Schließsystem mit Sicherheitsschlössern
- Dokumentierte Aus- und Rückgabe der Schlüssel

2.2 Zugangskontrolle Für die Rechner der Mitarbeitenden ebenso wie für eigene Server (bei Hetzner) unternimmt helpwave umfangreiche Maßnahmen, um die Nutzung durch Unbefugte zu verhindern:

- Alle nicht-öffentlichen Dienste sind grundsätzlich durch individuelle Benutzername/Passwort-Kombinationen geschützt.
- Die Anmeldung bei kritischen Diensten ist entweder
  - ausschließlich mit einem Benutzernamen und einem Sicherheitszertifikat oder mit
  - Benutzername, Passwort und Zwei-Faktor-Authentifizierung möglich, d.h. unser Verwendung eines zusätzlichen, getrennt generierten Einmaltokens. und erfolgt ausschließlich über gesicherte Verbindungen (bspw. SSH-Tunnel).
- Ein Zugriff auf Datenbanken der Kunden bzw. Anwendungsdaten erfolgt nur nach Aufforderung durch die Kunden und, sofern er nicht vor Ort erfolgt, nur mittels VPN, welches durch Superadmins/Admins gesichert wird. Sofern und soweit sich Daten dieser Kategorie auf Geräten der berechtigten Mitarbeiter befinden, sind diese vollverschlüsselt und sind nur nach Anmeldung durch den Nutzer entschlüsselbar, um einen Zugriff auf die Daten bei Verlust oder Diebstahl des Rechners zu verhindern.
- Die Festplatten der datenhaltenden Systeme im Rechenzentrum der Hetzner GmbH sind verschlüsselt.
- Kundenstammdaten, die sich auf den Geräten der Mitarbeiter zum Zwecke der Vertragserfüllung befinden, sind durch individuelle Benutzername/Passwort-Kombinationen geschützt.
- Alle Mitarbeitenden sind dazu angehalten, ihre Geräte in der jeweilis höchsten Sicherheitskonfiguration zu betreiben, unabhängig von ihrer konkreten Funktion i.S.d. oben beschriebenen Rollenkonzeption.
- Alle Mitarbeitenden sind dazu angehalten, zeitnah nach Veröffentlichung alle zur Verfügung gestellten Sicherheitsupdates zu installieren und das Betriebssystem der jeweiligen Geräte auf dem aktuellen Stand zu halten.
- Systeme sind von außen nur über die technisch notwendigen Ports zugreifbar. Verwaltungsports werden ausschließlich für die Zeit der Verwaltung (z. B. Wartung) freigeschaltet.

2.3 Zugriffskontrolle helpwave stellt sicher, dass Personen nur entsprechend der ihnen eingeräumten Zugriffsberechtigung auf IT-Systeme und die darauf gespeicherten Daten zugreifen können. Dies wird durch folgende Maßnahmen erreicht:

- Benutzer und ihre Zugriffsrechte werden zentral verwaltet, aktiviert und gesperrt.

- Ein Zugriff auf die datenhaltenden Systeme ist nur durch Superadmins und nach Freigabe durch Admins möglich.
- Die Verwaltung der Nutzer für sicherheits- und datenschutzrelevante Systeme ist nur für Superadmins und nach Freigabe für Admins möglich.
- Kennwörter sind mindestens 12 Zeichen lang, Passwörter für datenhaltende Systeme mindestens 64 Zeichen.
- Kennwörter werden ausschließlich mit einem Randomisierer erzeugt, damit keine Wörterbuch-Attacken auf diese möglich sind.
- Für die ordnungsgemäße Vernichtung von Dokumenten wird ein Aktenvernichter genutzt. Die Vernichtung alter Server in den Rechenzentren erfolgt nach deren Standard. Soweit unternehmenseigene Geräte nicht mehr weiter genutzt werden, werden sie mehrfach überschrieben und dann durch darauf spezialisierte Drittanbieter vernichtet.
- Physische Zugriffe auf datenhaltende Systeme im Rechenzentrum werden durch das Rechenzentrum protokolliert und automatisiert an die Geschäftsführung von helpwave mitgeteilt.

2.4 Trennungskontrolle Mit den folgenden Maßnahmen realisiert helpwave die Trennung der Daten verschiedener Kunden bzw. Kundenprojekte:

- Kundenprojekte werden, sofern erforderlich, auf jeweils eigenen Servern gespeichert
- Produktiv- und Testsysteme werden getrennt betrieben
- Alle angebotenen Produkte sind mandantenfähig, dass heißt, innerhalb einer einzelnen Anwendung erfolgt eine logische Trennung der Mandanten.

2.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO) helpwave gewährleistet, dass Datensätze bei der Datenübermittlung an Dritte pseudonymisiert und verschlüsselt werden.

3 Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

3.1 Weitergabekontrolle Daten zwischen Auftraggeber und Auftragnehmer werden, sofern nicht anders vom Auftraggeber gewünscht, ausschließlich elektronisch übertragen, d. h. ein Datentransport per Datenträger findet nicht statt. Sofern auf Wunsch des Auftraggebers ein Transport per Datenträger stattfindet, wird dieser vollständig verschlüsselt und das Passwort für die Entschlüsselung auf einem anderen Transportweg (bspw. persönlich oder per Telefon) mitgeteilt. Dementsprechend werden folgende Maßnahmen zur Sicherung der personenbezogenen Daten bei der Übertragung vorgenommen:

- Daten werden ausschließlich transport-verschlüsselt (per SSH-, SSL-, TLS v1.3 - oder VPN-Verbindung) übertragen.
- Falls Anwendungsdaten zur Demonstration von Funktionen der Anwendung benötigt werden (sogenannte Test-Daten), werden diese vor der Übertragung auf das Testsystem pseudonymisiert.
- Zugriffe auf die Systeme (außer über die Anwendung selbst) werden protokolliert.

3.2 Eingabekontrolle Folgende Maßnahmen gewährleisten die Überprüfung und Feststellung, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind:

- Im Rahmen der Anwendungsentwicklung und des Betriebs der Anwendung erfolgt keine Eingabe oder Änderung von Anwendungsdaten durch helpwave. Dies obliegt allein dem Auftraggeber.
- Das Löschen von Datensicherungsdateien im Rahmen des Betriebs erfolgt nach der vom Auftraggeber festgelegten Frist oder jährlich bzw. nach Vertragsende.

- Maßnahmen innerhalb der Anwendung, die die Nachvollziehbarkeit von Datenänderungen sicherstellen und Lösch- und Sperrfristen umsetzt, sind durch den Auftraggeber im Rahmen der Zusammenarbeit zu beauftragen oder – sofern technisch möglich – selbst in der Anwendung zu aktivieren.

3.3 Datenlöschung Auf der Grundlage eines umfassenden Löschkonzepts stellen wir sicher, dass personenbezogene sowie besonders sensible Gesundheitsdaten zur so lange gespeichert werden, wie es zur Erfüllung der jeweiligen Zwecke erforderlich ist. Die Löschung erfolgt nach Maßgabe der Art. 5 Abs. 1 lit e DS-GVO, Art. 17 DS-GVO und § 35 BDSG unter Berücksichtigung der dort genannten Ausnahmetatbestände.

Die Löschfristen orientieren sich an gesetzlichen Aufbewahrungsfristen und unterscheiden sich nach den Kategorien der zu löschenden Daten. Eine detaillierte Übersicht findet sich im Verarbeitungsverzeichnis. Darüber können der Wegfall des Verarbeitungszwecks oder der Widerruf der Einwilligung bzw. die Ausübung eines Löschrechts die Notwendigkeit einer Löschung ergeben.

Soweit möglich, werden Daten automatisiert nach den jeweils geltenden Löschfristen gelöscht. Der Vorgang der Löschung wird dokumentiert. Gleiches gilt für den Fall einer manuellen Löschung, welche nach Prüfung erfolgen kann.

Erfolgt eine Anfrage eines Betroffenen, erfolgt unverzüglich einer Prüfung derselben und, zielt sie auf Löschung ab, die Löschung der personenbezogenen Daten, soweit keine rechtlichen Aufbewahrungspflichten bestehen.

Kommt es zu einer Beendigung eines Vertragsverhältnis, können die zu löschenden Daten auf Anfrage zunächst in verschlüsselter Form den KundInnen zur Verfügung gestellt werden. Die dadurch entstehenden zusätzlichen Kosten müssen von den KundInnen übernommen werden.

Es erfolgt eine regelmäßige Überprüfung und Aktualisierung der Löschfristen und Prozesse. Manuelle Löschvorgänge sind nur durch Superadmins bzw. ggf. Admins möglich und werden protokolliert.

4 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

4.1 Verfügbarkeitskontrolle Die Verarbeitung personenbezogener Daten erfolgt in den Rechenzentrum von Hetzner und in den Büroräumen von helpwave.

4.1.1 Rechenzentrum Hetzner ist für den Serverbetrieb im Rechenzentrum vertraglich verpflichtet, mindestens mit den folgenden Maßnahmen die Verfügbarkeit sicherzustellen:
- Betrieb einer unterbrechungsfreien Stromversorgung
- Temperatur- Feuchtigkeits- und Klimaüberwachung
- Feuer- und Rauchmeldeanlagen
- Automatische Feuerlöschanlagen
- Vorhalten von Austauschgeräten zur schnellen Wiederherstellung bei Defekten

4.2 Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

4.2.1 Rechenzentrum Daten im Rechenzentrum der Deutschen Telekom werden zum Schutz vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung wie folgt gesichert:

- Nächtliche Sicherung aller Daten als Festplattenabbild (die Festplatten sind software-verschlüsselt).
- Backups werden 14 Tage rückwirkend vorgehalten.
- Nach Ablauf der Zeit werden die Daten unwiderruflich gelöscht, sofern vom Auftraggeber nichts anderes gewünscht wird.
- Datensicherungen befinden sich auf vom normalen Betrieb getrennten Systemen.
- Die Sicherung der Systeme erfolgt stets vollständig, um eine schnelle Wiederherstellung zu ermöglichen.
- Der vom normalen Betrieb getrennte Speicher wird mit denselben Vorkehrungen gesichert wie die Infrastruktur des normalen Betriebs: Selektive Zugriffe nur für notwendige Personen (Geschäftsführung). Erst bei einer Wiederherstellung der Daten wird die Sicherung außerhalb des Sicherungsspeichers wieder entschlüsselt.
- Die Übertragung der Sicherung zum speichernden System selbst erfolgt ebenfalls über eine verschlüsselte Verbindung. Die tägliche Datensicherung wird überwacht. Bei einem Fehler werden qualifizierte Mitarbeiter (Geschäftsführung) umgehend benachrichtigt. Um der Speicherbegrenzung gerecht zu werden, werden vor Inbetriebnahme einer wiederhergestellten Datensicherung die für personenbezogene Daten relevanten, automatisierten Sperr- und Löschregeln auf die Daten angewandt. Hierdurch wird sichergestellt, dass Daten, welche zwischenzeitlich gelöscht wurden aber in der Sicherung aber noch vorhanden waren, erneut gelöscht werden (Artikel 5 DSGVO).

4.2.2 Büroräume

- Die Sicherung von Daten erfolgt in verschlüsselter Form auf externen Datenträgern, die separat gelagert werden.
- Der Zugriff auf die Sicherungen ist nur mit einem Passwort möglich.
- Daten, die gesichert werden, umfassen keine Daten, die der Auftraggeber in die bereitgestellten Anwendungen eingegeben hat, sondern ausschließlich Daten zu Verträgen zwischen Auftraggeber und Auftragnehmer und zugehörigen Daten, die für die Erfüllung der Verträge erforderlich sind (z. B. Daten zu Supportanfragen).

5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Um zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend der Weisungen des Auftraggebers verarbeitet werden, unternimmt helpwave u.a. die folgenden Maßnahmen:

- Überprüfung vorhandener Zertifizierungen von Unterauftragnehmern (speziell gemäß ISO 27001)
- Abschluss einer Vereinbarung zur Auftragsdatenverarbeitung oder von EU- Standardvertragsklauseln
- Überprüfen von sonstigen Dokumentationen und Rechercheergebnissen, die eine Beurteilung der Zuverlässigkeit eines Anbieters ermöglichen

6 Datenschutz-Management (Art. 32 Abs. 4 DS-GVO)

helpwave bemüht sich grundsätzlich, nur Mitgliedern der Geschäftsführung den Zugang zu personenbezogenen Daten zu ermöglichen. Der Zugang zu Kunden- und Anwendungsdaten wird anderen Personen nur gewährt, sofern und soweit dies zwingend für die Vertragserfüllung oder Aufrechterhaltung der Funktionsfähigkeit der Anwendungen bzw. Systeme erforderlich ist. Sofern dies in Ausnahmefällen der Fall ist, gewährleistet helpwave, dass diese Personen die Daten nur auf Anweisung des Verantwortlichen bzw. des Auftragverarbeiters verarbeiten. Im Sinne eines umfangreichen Datenschutz-Management unternimmt helpwave folgende Maßnahmen:

- Die Bestellung eines externen Datenschutzbeauftragten ist erfolgt.
  Dr. Martina Zell, Zell Medical Consulting UG (haftungsbeschränkt)
  Herchenrath 30, 53804 Much
- Eine Datenschutz-Folgenabschätzung (DSFA) wurde durchgeführt und wird im u.g. Abständen aktualisiert
  Jährlich und ereignisbasiert (z.B. bei wesentlichen Anpassungen der Anwendungen, rechtlichen Änderungen oder Änderungen der einbezogenen Subunternehmer)
- Sofern und soweit helpwave Informationspflichten nach Art. 13 und 14 der DSGVO trifft, werden diese erfüllt.
- Ein Incident-Response-Management-System ist etabliert.
- Die Mitarbeiter sind dem Thema Datenschutz verpflichtet. Schulungs- und Sensibilisierungsmaßnahmen werden dokumentiert.
  Die Mitarbeiter werden nach den hier und dem Datenschutzkonzept dargelegten Grundsätzen auf die Einheitlich höchstmöglicher Vertraulichkeit verpflichtet.
  Es findet eine regelmäßige Sensibilisierung der Mitarbeiter zum Thema Datenschutz statt.
  Es erfolgt die Aufklärung über die Rechte und Pflichten im Umgang mit personenbezogenen Daten.
  Es erfolgt der Abschluss einer Vertraulichkeitsverpflichtung zwischen helpwave und den Personen.
- Ein Verzeichnis der Verarbeitungstätigkeiten ist erstellt und wird in u.g. Abständen aktualisiert.
  Jährlich und ereignisbasiert (z.B. bei wesentlichen Anpassungen der Anwendungen, rechtlichen Änderungen oder Änderungen der einbezogenen Subunternehmer)
- Die vorhandende IT-Infrastruktur sowie die eingesetzen Programme und Anwendungen werden dokumentiert.
- Die Wirksamkeit der technischen Schutzmaßnahmen, wie hier dargelegt, werden regelmäßig in u.g. Abständen überprüft.
  Jährlich und ereignisbasiert (z.B. bei wesentlichen Anpassungen der Anwendungen, rechtlichen Änderungen oder Änderungen der einbezogenen Subunternehmer)

7 Incident-Response-Management

Zum Schutz vor und im Falle von Sicherheitsvorfällen und Datenschutzverletzungen unternimmt helpwave die folgenden Maßnahmen:

- Alle Systeme sind durch eine Firewall geschützt, die von Hetzner zur Verfügung gestellt werden. Darüber hinaus nutzt helpwave GmbHteilweise eine zusätzliche Firewall.
- Zugriffe auf Verwaltungsports werden umgehend an die Geschäftsführung von helpwave gemeldet.

- Alle Mitarbeitenden sind verpflichtet, den Verdacht auf oder einen erfolgten unberechtigten Zugriff durch Dritte auf Geräte, auf denen sich personenbezogene Daten befinden könnten, der Geschäftsführung zu melden.
- Der Verdacht auf und im Fall von Sicherheitsvorfällen oder Datenschutzverletzungen werden diese dokumentiert und an die verantwortliche Stelle, den Datenschutzbeauftragten und, soweit vorgeschrieben, die gesetzlichen Aufsichtsbehörden gemeldet
- Im Anschluss an einen Sicherheitsvorfall wird dieser im Rahmen eines formalen Prozesses dokumentiert und betroffenen Kunden werden informiert.

8 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

helpwave stellt eine datenschutzfreundliche Technikgestaltung wie folgt sicher:

- Die über das Kommunikationssystems von helpwave geführten Chatverläufe erfolgen sind stets verschlüsselt (Zwei-Wege-Kommunikation).
- Ein Rollenkonzeption zur Einschränkung des Datenzugriffs und zu Beschränkung von Benutzerrechten ist eingerichtet worden.
- Zugriffsrechte sind automatisch an die verschiedenen Benutzerrollen angepasst bzw. beschränkt.
- Zugriffsrechte der Mitarbeiter von helpwave auf Endgeräte, die an das Netzwerk von helpwave angeschlossen sind, sind automatisch beschränkt. Alle Endgeräte sind verschlüsselt und können zudem nur mit Benutzername und Passwort genutzt werden.
- Es werden ausschließlich Daten erhoben, die für die Zwecke der Vertragserfüllung oder den technischen Betrieb der zur Verfügung gestellten Anwendungen erforderlich sind („Datensparsamkeit“).

9 Auftragskontrolle

Die Auftragskontrolle umfasst Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen verarbeitet werden können. Diese Maßnahmen umfassen bei helpwave:

- Alle Mitarbeiter der helpwave sind angewiesen, nur nach den vereinbarten Vertragsinhalten zu arbeiten.
- Alle bereitgestellten Daten verbleiben ausschließlich in der Verfügungsmacht der helpwave.
- Eine Weitergabe personenbezogener Daten erfolgt nur mit Zustimmung der KundInnen und nur Maßgabe der hier genannten Maßnahmen und im Rahmen datenschutzrechtlicher Bestimmungen.
- Dienstleister der helpwave unterliegen einer laufenden Überprüfung gemäß Abschnitt 4.
- Alle Mitarbeiter der helpwave, die mit personenbezogenen Daten aus dem Bereich der Auftraggeber in Kontakt kommen könnten, sind schriftlich auf die Einhaltung des Datenschutzes verpflichtet. Sie sind entsprechend belehrt und angewiesen, dass sie Arbeiten gemäß dem vorstehenden Absatz nur auf Anforderung des Auftraggebers durchführen dürfen.