Technische und organisatorische Maßnahmen (TOM)

i.S.d. Art. 32 DSGVO

helpwave GmbH
c/o Collective Incubator, 3. OG
Jülicher Straße 209d
52070 Aachen
NRW Deutschland
Aachen HRB 27480

20. Dezember 2024

Inhaltsverzeichnis

Die Anwendungsdaten werden in zwei verschiedenen Räumlichkeiten verarbeitet, im Büro der helpwave GmbH (im Folgenden „helpwave“) und in von Unterauftragnehmern zur Verfügung gestellten Rechenzentren. helpwave nutzt für den Betrieb der datenhaltenden Server das Rechenzentrum der Open Telekom Cloud der Telekom Deutschland GmbH (im Folgenden „Deutsche Telekom“), die Unterauftragnehmer von helpwave ist. Für einzelne Anwendungen werden zudem Abschottungssysteme (Gatekeeper oder Load-Balancer) eingesetzt, um den Standort der eigentlichen Datenhaltungssysteme zu verschleiern. Hierfür werden Systeme im Rechenzentrum der Firma Hetzner eingesetzt. Diese leiten die Daten jedoch nur in verschlüsselter Form (SSL) an die Systeme bei der Deutschen Telekom weiter. Nachfolgende Ausführungen zum Bereich „Rechenzentrum“ beziehen sich immer sowohl auf das Rechenzentrum der Deutschen Telekom, als auch auf das bei Hetzner. 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:

- Deutsche Telekom: www.telekom.com
- Hetzner: www.hetzner.com

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

1.1 Zutrittskontrolle

1.1.1 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.

1.1.2 Buroräume Die Büroräume der helpwave GmbH liegen im 3. OG in der Jülicher Straße 209d in 52070 Aachen. In diesen Büroräumen befinden sich keine stationären Datenverarbeitungsanlagen, die zur Verarbeitung von Daten der Kunden von helpwave genutzt werden. Die Verarbeitung erfolgt ausschließlich auf mobilen Geräten mit besonderen Schutzmechanismen und nur durch autorisierte Personen. Der Zugang zu den Büroräumen ist durch folgende Maßnahmen geschützt:

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

1.2 Zugangskontrolle Für die Rechner der Mitarbeitenden ebenso wie für eigene Server (bei der Deutschen Telekom/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 externer Zugang zum Büronetzwerk ist nicht möglich.
- Sofern die Mitarbeitenden firmeneigene Smartphones nutzen, sind diese durch Vollverschlüsselung geschützt und können bei Diebstahl oder Verlust aus der Ferne gelöscht werden.
- Die Daten auf den Rechnern der Mitarbeitenden sind vollständig verschlüsselt und 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 Deutschen Telekom sind verschlüsselt.
- Kundendaten, die sich auf den Geräten der Mitarbeiter zum Zwecke der Vertragserfüllung befinden, sind in einem zusätzlich verschlüsselten Dateicontainer gespeichert.
- Durch den ausschließlichen Einsatz von Apple-Computern, auf denen zeitnah nach einer Veröffentlichung alle zur Verfügung gestellten Sicherheitsupdates installiert werden, reduzieren sich die Angriffsmöglichkeiten auf die Systeme deutlich.
- Systeme sind von außen nur über die technisch notwendigen Ports zugreifbar. Verwaltungsports werden ausschließlich für die Zeit der Verwaltung (z. B. Wartung) freigeschaltet.

1.3 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 die Geschäftsführung möglich.
- Die Verwaltung der Nutzer für sicherheits- und datenschutzrelevante Systeme ist nur für die Geschäftsführung möglich.
- Kennwörter sind mindestens 12 Zeichen lang, Passwörter für datenhaltende Systeme
- mindestens 30 Zeichen.
- Kennwörter werden ausschließlich mit einem Randomisierer erzeugt, damit keine Wörterbuch-Attacken auf diese möglich sind.
- Kennwörter werden mindestens alle 3 Monate geändert.
- Für die ordnungsgemäße Vernichtung von Dokumenten und optischen Datenträgern wird ein Aktenvernichter genutzt.
- Zugriffe auf datenhaltende Systeme im Rechenzentrum werden durch das Rechenzentrum protokolliert und automatisiert an die Geschäftsführung von helpwave mitgeteilt. Das beinhaltet den reinen Zugriff ebenso wie Änderung von Firewall-Konfigurationen, wie bspw. das Aktivieren und Deaktivieren von Verwaltungsports auf einzelnen Systemen.

1.4 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.

1.5 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.

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

2.1 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- 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.

2.2 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 standardmäßig nach 14 Tagen.
- Maßnahmen innerhalb der Anwendung, die die Nachvollziehbarkeit von Datenänderungen sicherstellt 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 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

3.1 Verfügbarkeitskontrolle Die Verarbeitung personenbezogener Daten erfolgt im Rechenzentrum der Deutschen Telekom und in den Büroräumen von helpwave. Bei Hetzner erfolgt aus Sicherheitsgründen eine Durchleitung der Daten zur Deutschen Telekom, es werden hier aber keine Daten gespeichert. Dementsprechend sind beim Schutz personenbezogener Daten vor zufälliger Zerstörung oder Verlust die Maßnahmen für die beiden Standorte (Deutsche Telekom/Büroräume helpwave) zu unterscheiden.

3.1.1 Rechenzentrum Die Deutsche Telekom/Hetzner sind 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 Löschanlagen
- Vorhalten von Austauschgeräten zur schnellen Wiederherstellung bei Defekten

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

3.2.1 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.
- Datensicherungen von datenhaltenden Festplatten sind verschlüsselt.

- 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 wir sichergestellt, dass Daten, welche zwischenzeitlich gelöscht wurden aber in der Sicherung aber noch vorhanden waren, erneut gelöscht werden (Artikel 5 DSGVO).

3.2.2 Büroräume

- Daten, die sich auf Geräten innerhalb der Räumlichkeiten von helpwave oder auch außerhalb auf mobilen Geräten der Geschäftsführung befinden, werden mindestens 2 Mal wöchentlich gesichert.
- Die Sicherung 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).

4 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
- Kontrolle der Vertragsausführung

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

helpwave bemüht sich grundsätzlich, nur Mitgliedern der Geschäftsführung den Zugang zu personenbezogenen Daten zu ermöglichen. Sofern jedoch in Ausnahmefällen die Mitarbeit anderer Personen oder freier Mitarbeiter (die ggf. Zugang zu personenbezogenen Daten haben) erforderlich ist, gewährleistet helpwave, dass diese die Daten nur auf Anweisung des Verantwortlichen bzw. des Auftragverarbeiters verarbeiten und unternimmt hierzu folgende Maßnahmen:

- Aufklärung über die Rechte und Pflichten im Umgang mit personenbezogenen Daten.
- Abschluss einer Vertraulichkeitsverpflichtung zwischen helpwave und den Personen.
- Regelmäßige Schulungen im Umgang mit personenbezogenen Daten.

6 Incident-Response-Management

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

- Alle Systeme sind durch eine Firewall geschützt, die von der Deutschen Telekom bzw. Hetzner zur Verfügung gestellt werden.
- Zudem werden die Systeme durch ein Anti-DDoS-System vor sog. Denial-Of-Service- Attacken geschützt.
- Zugriffe auf Verwaltungsports werden umgehend an die Geschäftsführung von helpwave gemeldet.
- Sicherheitsverletzungen werden umgehend an Anwählte und Experten weitergeleitet, die im Rahmen einer extra für diesen Fall abgeschlossenen Versicherung durch die Provinzial in Münster (Cyber-Police) zur Verfügung gestellt werden. Im Rahmen der Versicherung werden gemäß der Vorgaben der DS-GVO entsprechende, kurzfristige Meldungen an die Aufsichtsbehörden durchgeführt und Anlaufstellen für betroffene Kunden eingerichtet. Zudem werden forensische Dienstleister mit der Untersuchung des Vorfalls beauftragt. Entsprechende weitere, beratende Personen (bspw. der uns in Datenschutzfragen beratende Anwalt Herr Dr. Eduard Wessel, Münster) werden informiert und konsultiert.
- Im Anschluss an einen Vorfall wird dieser im Rahmen eines formalen Prozesses dokumentiert und betroffenen Kunden werden informiert. 7. 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. Darüber hinaus verwendet helpwave datenschutzfreundliche Voreinstellungen, die durch folgende Maßnahmen gewährleistet werden:
- Im Rahmen des Kommunikationssystems von helpwave werden Chatverläufe automatisch verschlüsselt gespeichert.

- 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 können nur im Besitz von helpwave befindliche Endgeräte für die tägliche Arbeit und Vertragserfüllung 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“).

7 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.
- Weitergabe personenbezogener Daten erfolgt im Rahmen der datenschutzrechtlichen 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.