

# Sicherheit auf einen Blick

HelpYa ist ein digitaler Pager. Gäste, Kunden oder Patienten werden über ihr eigenes Handy benachrichtigt, wenn sie an der Reihe sind. Für die Nummer braucht HelpYa von den Wartenden keinen Namen, keine Telefonnummer und kein Konto. Dieses Blatt beschreibt, wie wir die Daten unserer Kunden schützen.

## HOSTING UND STANDORT

- Rechenzentrum: Hetzner Online GmbH (Nürnberg/Falkenstein) – ISO/IEC 27001:2022 zertifiziert und mit BSI-C5-Testat (C5:2020 Typ 2) für die genutzten Cloud- und Speicherdienste.
- Laufende Kopie der Datenbank an einem zweiten Hetzner-Standort in Deutschland. Nächtliche, verschlüsselte Sicherung bei einem zweiten Anbieter in der EU (Frankreich).
- Alle Unterauftragsverarbeiter stehen im Auftragsverarbeitungsvertrag (AVV), Anlage 2.
- Für Rahmenverträge bieten wir eine vertraglich zugesicherte Verfügbarkeit (SLA) an.

## VERSCHLÜSSELUNG

- Jede Verbindung läuft über HTTPS (TLS). HSTS verhindert unverschlüsselte Aufrufe.
- Push-Mitteilungen sind Ende-zu-Ende verschlüsselt nach dem Web-Push-Standard (RFC 8291). Die Push-Dienste von Apple, Google und Mozilla sehen den Inhalt nicht.
- Passwörter speichern wir nur als PBKDF2-Hash mit 600.000 Runden. Anmelde-Codes, Geräte-Token und Kassen-Schlüssel speichern wir nur als Prüfsumme. Zugangsdaten zu Zahlungsanbietern sind gesondert verschlüsselt.
- Die Datenbank liegt auf einem eigenen, im Ruhezustand verschlüsselten Datenträger (LUKS2, AES-256).
- Die laufende Kopie der Datenbank und die Offsite-Sicherungen sind verschlüsselt; der Schlüssel zur laufenden Kopie liegt nicht auf dem Server.

## ZUGRIFF UND ROLLEN

- Strikte Trennung der Daten je Kunde: Jeder Zugriff ist an den eigenen Betrieb gebunden.
- AnmeldeLinks für Geräte werden nur als Prüfsumme gespeichert; QR-Codes zum Koppeln gelten 30 Minuten.
- Single Sign-on per OpenID Connect (z. B. Microsoft Entra ID, Google Workspace), je Betrieb einstellbar, optional ausschließlich per SSO. SSO-Sitzungen enden nach 12 Stunden; wer im Firmenkonto deaktiviert wird, verliert so spätestens dann den Zugang. Anmeldungen werden protokolliert.
- Rollen im Betrieb: Admin (alles) und Mitarbeiter (nur Arbeitsansichten). Theken-Geräte sind einzeln angemeldet und einzeln widerrufbar. Die Kassenanbindung läuft über einen eigenen Schlüssel je Betrieb, Webhooks sind signiert.
- Gäste- und Patientendaten sieht HelpYa nur mit Ihrer Freigabe (Code, höchstens 60 Minuten, nur ansehen oder ändern); jeder Zugriff wird protokolliert und ist im Kundenbereich einsehbar. Verwaltungszugänge sind persönlich und mit zweitem Faktor gesichert.

## KONTEN-SICHERHEIT

- Zwei-Faktor-Anmeldung für jedes Konto mit Passwort: per Code aus der E-Mail oder per Authenticator-App (TOTP) mit Ersatzcodes.
- Schutz gegen Durchprobieren von Passwörtern und Codes.
- Sitzungen laufen nach Inaktivität ab. Ein Passwortwechsel meldet alle Sitzungen ab. Cookies sind auf HTTPS beschränkt und für Skripte nicht lesbar.

## DATENSIPARSAMKEIT

- Für die Nummer braucht HelpYa keinen Namen, keine Telefonnummer und kein Konto der Wartenden. Wo eine Funktion mehr braucht, etwa einen Namen für die Vorbestellung oder einen freiwilligen Kontakt am Messestand, steht es bei der Funktion.
- Abgeschlossene Nummern werden nach 24 Stunden automatisch anonymisiert. Weitere feste Löschfristen stehen im AVV Nr. 9.
- Keine Werbe-Tracker, keine Analyse-Werkzeuge, keine Inhalte Dritter.

## SICHERUNG UND WIEDERHERSTELLUNG

- Laufende Kopie der Datenbank im Abstand von Sekunden. Nächtliche verschlüsselte Sicherung. Zusätzliche Sicherung vor jeder Softwareänderung.
- Die Wiederherstellung aus der Offsite-Sicherung wird monatlich automatisch geprüft.
- Sicherungen werden höchstens 30 Tage aufbewahrt; Server-Protokolle nach 14 Tagen gelöscht. Sicherungen dienen nur der Wiederherstellung (AVV Nr. 9 Abs. 3).

## BETRIEB UND UPDATES

- Die Anwendung läuft isoliert in einem Container ohne Administratorrechte, in einem eigenen Netz und mit Ressourcengrenzen.
- Der Server ist nur mit kryptografischem Schlüssel erreichbar. Die Passwort-Anmeldung ist abgeschaltet, wiederholte Fehlversuche werden gesperrt. Sicherheitsupdates des Betriebssystems werden automatisch eingespielt.
- Softwarestände sind festgelegt und werden nur aus geprüften Versionen ausgerollt. Die Erreichbarkeit wird rund um die Uhr extern überwacht.
- Abhängigkeiten werden vor jedem Ausrollen automatisch auf bekannte Schwachstellen geprüft.
- Hochgeladene Dateien (Bilder, PDFs, Kostenvoranschläge, Speisekarten) werden vor dem Speichern auf Schadsoftware geprüft; befallene Dateien werden abgewiesen. Ist die Prüfung nicht verfügbar, werden PDFs und Kostenvoranschläge nicht angenommen.
- Änderungen werden vor dem Livegang automatisch in einer abgeschotteten Testumgebung mit Testdaten geprüft; Ausnahmen nur bei dringenden Sicherheitskorrekturen und dokumentiert.
- Entwickelt wird nur mit Testdaten.

## VORFALLMANAGEMENT

- Datenschutzverletzungen melden wir dem Kunden unverzüglich, spätestens innerhalb von 24 Stunden nach Bekanntwerden, mit den Angaben nach Art. 33 Abs. 3 DSGVO, soweit bekannt (AVV Nr. 8).
- Sicherheitslücken bitte vertraulich an [kontakt@helpya.com](mailto:kontakt@helpya.com) melden (Meldeweg: [helpya.com/sicherheitsluecke-melden](https://helpya.com/sicherheitsluecke-melden); maschinenlesbar: [helpya.com/.well-known/security.txt](https://helpya.com/.well-known/security.txt)).

## UNTERAUFTRAGSVERARBEITER

- Vollständige Liste mit Zweck und Sitz: AVV Anlage 2 unter [helpya.com/avv](https://helpya.com/avv). Gästedaten bleiben in der EU, mit Ausnahme der verschlüsselten Push-Zustellung über die Dienste der Gerätehersteller.

## IN UMSETZUNG

- Strenge Content-Security-Policy gegen eingeschleuste Skripte – derzeit im Prüfbetrieb, Scharfschaltung geplant.
- Zweiter Server an einem anderen Standort mit automatischem Umschalten; danach zugesicherte Verfügbarkeit (SLA) in allen Tarifen.

## ANSPRECHPARTNER

- Sicherheit und Datenschutz: [kontakt@helpya.com](mailto:kontakt@helpya.com) · Verantwortlich: Geschäftsführung der FFM&M RE GmbH

Weitere Unterlagen (ausgefüllte Fragebögen, technische Details) geben wir auf Anfrage unter Vertraulichkeitsvereinbarung heraus.