LENVAR
DER DIGITALE MITARBEITER

Stand: November 2026

Technische und organisatorische Maßnahmen

Anlage 1 zum Vertrag zur Auftragsverarbeitung. Die LWO Digital GmbH trifft für LENVAR die folgenden Maßnahmen nach Art. 32 DSGVO. Sie werden weiterentwickelt, ohne das Schutzniveau zu unterschreiten.

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

Bereich	Maßnahme
Zutritt	Die Server stehen im Rechenzentrum der Hetzner Online GmbH in Deutschland. Zutritt und physische Sicherung regelt der Rechenzentrumsbetreiber nach seinem Vertrag zur Auftragsverarbeitung. Der Auftragsverarbeiter betreibt keine eigenen Serverräume.
Zugang zu Systemen	Von außen erreichbar sind nur die verschlüsselten Web-Zugänge (Ports 80 und 443 über einen vorgeschalteten Webserver). Die Anwendung selbst ist nur intern erreichbar. Eingänge von Dienstleistern (Telefonie, Sprache, SMS, Mail) werden nur angenommen, wenn deren Signatur oder ein geheimer Schlüssel stimmt; der Vergleich erfolgt zeitkonstant.
Zugriff auf Anfragen	Anfragen sind für Betrieb und Anfragende nur über zufällige, nicht erratbare und befristete Links erreichbar (Upload-Link 24 Stunden, Anfrage-Seite und Lese-Link für das Büro 7 Tage). Webseiten-Anfragen werden nur mit einem geheimen Schlüssel je Betrieb angenommen.
Trennung	Jeder Betrieb hat eine eigene Konfiguration und Kennung. Alle Daten sind dem Betrieb zugeordnet und werden nur für ihn abgefragt und ausgegeben. Daten werden nicht zwischen Betrieben geteilt; ausgenommen ist ein Widerspruch eines Anfragenden gegen SMS (STOP), der zu seinem Schutz für alle Betriebe gilt.
Pseudonymisierung und Datensparsamkeit	In technischen Protokollen stehen Telefonnummern nur mit den letzten drei Ziffern, Namen als Initialen, E-Mail-Adressen nur mit der Domain und Freitexte gekürzt. Zähler zum Schutz vor Missbrauch arbeiten mit Hashwerten statt mit Klardaten.
Personal	Zugriff auf die Systeme hat nur, wer ihn für Betrieb, Wartung und Fehlerbehebung braucht. Alle Beteiligten sind auf Vertraulichkeit verpflichtet.

2. Integrität

Bereich	Maßnahme
Weitergabe	Alle Seiten und Schnittstellen laufen nur verschlüsselt über HTTPS (TLS, Zertifikate über Let's Encrypt). Die Dienstleister werden über ihre verschlüsselten Schnittstellen angesprochen.
Eingabe	Eingänge werden mit Zeitpunkt und Herkunft als Ereignis am Vorgang protokolliert. Rohdaten eingehender Gesprächsdaten werden zur Fehlersuche höchstens 7 Tage aufbewahrt.

3. Verfügbarkeit und Belastbarkeit

Bereich	Maßnahme
Datensicherung	Datenbank und Fotos werden täglich gesichert. Gelöschte Daten können bis zum Ablauf der Sicherungsfrist in Sicherungen enthalten sein, höchstens 12 Monate; sie werden nur zur Behebung von Störungen wiederhergestellt.

Bereich	Maßnahme
Belastbarkeit	Anfragen an öffentliche Seiten und Eingänge sind je Minute begrenzt, um Missbrauch und Überlastung abzuwehren.
Wiederherstellung	Für den Ausfall des Servers gibt es eine dokumentierte Anleitung zur Wiederherstellung aus der Sicherung.

4. Löschung und Datensparsamkeit

Bereich	Maßnahme
Automatische Anonymisierung	Ein täglicher Löschlauf anonymisiert abgeschlossene Anfragen nach 90 Tagen oder nach der mit dem Betrieb vereinbarten Frist. Entfernt werden Name, Telefonnummer, E-Mail-Adresse, Straße, Beschreibung, Gesprächstext, Nachrichten und Fotos; übrig bleiben Ort, Art und Zeitpunkte der Anfrage für die Statistik.
Gedächtnis	Kontakte für das Wiedererkennen früherer Anfragen werden mit derselben Frist gelöscht, sofern der Betrieb keine eigene Frist festlegt.
Tonaufnahmen	Die Speicherung von Tonaufnahmen der Gespräche ist ausgeschaltet. Es bleibt der Gesprächstext. Sprachnachrichten (falls Messenger gebucht) werden nur bis zur Abschrift zwischengespeichert, höchstens 24 Stunden.
Kein Tracking	Die Seiten für Anfragende setzen keine Cookies, laden keine Pixel und keine Skripte fremder Anbieter.

5. Organisation und Überprüfung

Bereich	Maßnahme
Auftragskontrolle	Mit allen Unterauftragsverarbeitern (Anlage 2) bestehen Verträge zur Auftragsverarbeitung nach deren Standardbedingungen; Übermittlungen in Drittländer stützen sich auf die dort genannten Garantien.
Transparenz	LENVAR sagt zu Beginn jedes Anrufs, dass ein digitaler Mitarbeiter des Betriebs spricht. Die Seiten für Anfragende weisen auf die KI-Unterstützung hin.
Datenpannen	Meldeweg: kontakt@lenvar.de. Verletzungen werden dokumentiert und dem Betrieb nach § 8 Absatz 3 gemeldet.
Überprüfung	Die Maßnahmen werden bei jeder wesentlichen Änderung der Technik und mindestens einmal jährlich überprüft und angepasst.