

Anlage 2 zum AVV - Technische und organisatorische Maßnahmen

nach Art. 32 DSGVO Version 1.0 - Stand 11.09.2026

Der Auftragnehmer betreibt zwei Hosting-Plattformen. Die Verantwortung für die technischen Maßnahmen ist je Plattform unterschiedlich verteilt; beide sind nachfolgend getrennt beschrieben.

Plattform	Verwendung	Serverbetrieb	Anwendungsebene
A - Cloud Server mit Container-Plattform	Eigenentwickelte Websites und Anwendungen (z. B. Next.js), automatisiertes Deployment aus Git	Auftragnehmer	Auftragnehmer
B - Managed Server (Hetzner MC50)	Manuell installierte Content-Management-Systeme und Shops (z. B. WordPress, Contao, TYPO3) sowie statische Websites	Hetzner Online GmbH	Auftragnehmer

Beide Plattformen stehen ausschließlich in Rechenzentren der Hetzner Online GmbH in Deutschland. Physische Sicherheit und Infrastruktur verantwortet Hetzner; die Maßnahmen sind in Hetzners Anlage 2 zum Auftragsverarbeitungsvertrag (Version 1.2 vom 16.02.2026) sowie unter <https://docs.hetzner.com/de/general/others/technical-and-organizational-measures> beschrieben.

Hetzner weist ausdrücklich darauf hin, dass bei Cloud Servern die Verantwortung für Verwaltung, Wartung und Sicherheit der Serverinfrastruktur beim Auftragnehmer liegt. Beim Managed Server übernimmt Hetzner Betriebssystem, Serverdienste, Sicherheitsupdates der Infrastruktur, eine providerverwaltete Firewall mit 24/7-Monitoring sowie Backup und Wiederherstellung; die Pflege und Aktualität der aufgespielten Software bleibt in beiden Fällen beim Auftragnehmer.

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

Zutrittskontrolle

- Rechenzentrum (beide Plattformen): elektronisches Zutrittskontrollsystem mit Protokollierung, flächendeckende Videoüberwachung, Hochsicherheitszaun, Besucherregelung und Sicherheitsdienst durch Hetzner (ISO/IEC 27001, BSI C5 Typ 2)
- Arbeitsplatz des Auftragnehmers: abschließbare Büroräume, keine Server vor Ort, Geräte mit Festplattenverschlüsselung (FileVault) und Bildschirmsperre

Zugangskontrolle

Plattform A (Cloud Server):

- Server-Zugang ausschließlich per SSH mit Schlüsselpaaren, Passwort-Login deaktiviert
- Firewall: Aus dem öffentlichen Netz sind ausschließlich die Ports 80 (HTTP, Weiterleitung auf HTTPS) und 443 (HTTPS) erreichbar. SSH (22), Datenbankdienste (u. a. 5432), die Docker-Schnittstelle (2375/2376) und weitere Dienstports werden von der Firewall verworfen. Geprüft am 11.09.2026 durch Portprüfung von außen.
- Die Verwaltungsoberfläche der Deployment-Plattform ist ausschließlich über HTTPS erreichbar, nicht über einen offenen Verwaltungsport

Plattform B (Managed Server):

- Administrativer Zugriff auf Betriebssystem und Serverdienste erfolgt ausschließlich durch autorisierte

Beschäftigte der Hetzner Online GmbH über mehrstufige Authentifizierung

- Providerverwaltete Firewall mit 24/7-Monitoring durch Hetzner
- Zugang des Auftragnehmers über ein persönliches Kundenkonto mit Passwortpflicht und Zwei-Faktor-Authentifizierung sowie über SSH mit Schlüsselpaar
- Zugriffs- und Änderungsvorgänge im Kundenkonto werden von Hetzner protokolliert

Beide Plattformen:

- Zwei-Faktor-Authentifizierung für Hetzner-Konto, Deployment-Plattform, Quellcodeverwaltung und E-Mail
- Passwort-Manager mit individuellen, langen Passwörtern; keine geteilten Konten
- Automatische Sperre nach Fehlversuchen, Protokollierung von Anmeldungen

Zugriffskontrolle

- Plattform A: Zugriff auf die Container-Plattform nur für den Auftragnehmer; Kundenzugänge nur auf ausdrücklichen Wunsch und beschränkt auf das jeweilige Projekt. Administrative Tätigkeiten über einen personalisierten Account mit sudo, Root-Login deaktiviert.
- Plattform B: Jede Website erhält einen eigenen Systembenutzer mit eigenem Verzeichnisbaum und eigener Datenbank; Dateirechte werden restriktiv gesetzt. Für die Vergabe von Dateizugriffsrechten ist nach Hetznern Maßgabe der Auftragnehmer verantwortlich.
- Anwendungsebene: Redaktions- und Administratorkonten der Content-Management-Systeme werden personalisiert vergeben, nach dem Prinzip der geringsten Rechte eingerichtet und beim Ausscheiden von Personen entzogen
- Protokollierung administrativer Zugriffe

Trennungskontrolle

- Plattform A: Jede Kundenanwendung läuft in eigenen Containern mit eigenem Netzwerk, eigenen Datenträgern und eigener Konfiguration; keine gemeinsame Datenbank zwischen Kunden
- Plattform B: Trennung je Website über eigene Systembenutzer, getrennte Verzeichnisse und getrennte Datenbanken mit eigenen Zugangsdaten
- Getrennte Domains, Zertifikate und Zugangsdaten je Kunde; Test- und Produktivumgebungen sind getrennt
- Hetzner trennt auf beiden Plattformen zusätzlich Daten und Sicherungsdaten unterschiedlicher Kunden physisch und logisch

Pseudonymisierung und Verschlüsselung

- Transportverschlüsselung: ausschließlich HTTPS (TLS 1.2/1.3) mit automatisch erneuerten Zertifikaten, HTTP wird auf HTTPS umgeleitet; gilt für beide Plattformen
- Administrative Verbindungen ausschließlich verschlüsselt (SSH, HTTPS)
- Verschlüsselung ruhender Daten: Die Hetzner Online GmbH verschlüsselt gespeicherte Daten nicht; dies liegt nach deren Anlage 2 in der Verantwortung des Auftragnehmers. Der Schutz ruhender Daten erfolgt daher über Zutritts-, Zugangs- und Zugriffskontrolle sowie die physische Sicherheit des Rechenzentrums.
- Sicherungen des Managed Servers werden von Hetzner verschlüsselt abgelegt. Sicherungen des Cloud Servers werden nicht verschlüsselt gespeichert; sie liegen innerhalb derselben abgesicherten Infrastruktur und sind vom Produktivsystem getrennt.
- Protokolle werden nur als Laufzeitprotokolle vorgehalten. Auf Plattform A rotieren sie größenbasiert, je Dienst höchstens 10 MB in bis zu drei Dateien. Auf Plattform B gilt die Protokollierung der Hetzner Online GmbH; der Auftragnehmer greift dort nicht ein. In beiden Fällen legt der Auftragnehmer kein Langzeitarchiv an, wertet Protokolle nicht aus und führt sie nicht mit anderen Datenquellen zusammen.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle

- Datenübertragung zwischen Nutzern und Server ausschließlich verschlüsselt
- Kein Einsatz externer Analyse-, Tracking- oder Werbedienste durch den Auftragnehmer; solche Dienste werden nur auf ausdrückliche Weisung des Auftraggebers eingebunden
- Datenträger werden vor Entsorgung sicher gelöscht; im Rechenzentrum durch Hetzner nach einem definierten Verfahren, bei erfolgloser Löschung durch physische Zerstörung

Eingabekontrolle

- Plattform A: Änderungen an Code und Konfiguration ausschließlich über versionierte Git-Repositories mit vollständiger Historie; Deployments werden mit Zeitstempel, Commit und Ergebnis protokolliert
- Plattform B: Änderungen an Inhalten und Konfiguration erfolgen über die personalisierten Konten der jeweiligen Anwendung; die Content-Management-Systeme protokollieren Änderungen und die handelnde Person
- Serverkonfigurationen sind dokumentiert; Änderungen werden nachvollziehbar festgehalten

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b, c DSGVO)

Verfügbarkeitskontrolle

- Rechenzentrum: redundante Stromversorgung, freie Kühlung und Klimaanlage, Brandfrüherkennung mit automatischer Alarmierung, redundante Netzanbindung, dauerhaft aktive DDoS-Erkennung durch Hetzner
- Backups: Beide Plattformen werden über die Backup-Funktion der Hetzner Online GmbH gesichert. Plattform A (Cloud Server): tägliche Sicherung des gesamten Serverabbaus, sieben Sicherungsstände werden vorgehalten, der älteste wird beim Erstellen eines neuen überschrieben. Plattform B (Managed Server): tägliche Sicherung von Dateien und Datenbanken mit einer Aufbewahrung von bis zu 14 Tagen. Die Sicherungen werden logisch und physisch getrennt vom Produktivsystem gespeichert.
- Plattform B zusätzlich: Festplattenspiegelung sowie Virens Scanner und Sicherheitsprüfungen durch Hetzner
- Monitoring: Beim Managed Server überwacht Hetzner das System und meldet nach einem Eskalationskonzept (Meldung ab 80 %, dringende Meldung ab 90 % Speicherbelegung). Beim Cloud Server überwacht Hetzner nur den Host; die Überwachung des virtuellen Servers und der Anwendungen liegt beim Auftragnehmer und erfolgt durch Erreichbarkeitsprüfung mit Benachrichtigung.
- Aktualisierung: Betriebssystem und Serverdienste auf Plattform B durch Hetzner; auf Plattform A durch den Auftragnehmer. Content-Management-Systeme, Erweiterungen und Anwendungsabhängigkeiten werden auf beiden Plattformen vom Auftragnehmer regelmäßig aktualisiert, sicherheitskritische Aktualisierungen zeitnah.
- Schutz vor Überlast und Angriffen: Auf beiden Plattformen ist die DDoS-Erkennung der Hetzner Online GmbH dauerhaft aktiv. Plattform B zusätzlich über die providerverwaltete Firewall mit 24/7-Monitoring.

Wiederherstellbarkeit

- Plattform A: Wiederherstellung aus einem der sieben Sicherungsstände oder vollständiges Neu-Deployment aus dem Git-Repository
- Plattform B: Wiederherstellung aus der Hetzner-Sicherung von Dateien und Datenbanken, rückwirkend bis zu 14 Tage
- Das Vorgehen ist dokumentiert und wurde erprobt; es wird nach wesentlichen Änderungen an der Infrastruktur erneut geprüft

- Vereinbarte Reaktions- und Wiederherstellungszeiten ergeben sich aus dem Hauptvertrag

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

Datenschutz-Management

- Verzeichnis der Verarbeitungstätigkeiten für Auftragsverarbeiter wird geführt und jährlich geprüft
- Alle Personen mit Zugriff sind auf Vertraulichkeit verpflichtet
- Diese Maßnahmen werden mindestens jährlich sowie bei wesentlichen Änderungen der Infrastruktur überprüft

Incident-Response-Management

- Prozess zur Erkennung, Bewertung und Meldung von Sicherheitsvorfällen (siehe Dokument „Prozess Datenpanne“); Meldung an den Auftraggeber innerhalb von 24 Stunden
- Sicherheitsmeldungen der eingesetzten Software werden verfolgt; das betrifft insbesondere die Content-Management-Systeme und deren Erweiterungen, da diese die häufigste Angriffsfläche darstellen

Datenschutzfreundliche Voreinstellungen

- Websites werden ohne Tracking, ohne Cookies und ohne externe Ressourcen ausgeliefert, sofern der Auftraggeber nichts anderes beauftragt
- Schriften und weitere Einbindungen werden, soweit möglich, lokal ausgeliefert
- Protokolle werden auf das technisch Notwendige beschränkt

Auftragskontrolle

- Verarbeitung nur auf Weisung; Unterauftragsverarbeiter werden vor Beauftragung geprüft und in Anlage 3 geführt
- Mit der Hetzner Online GmbH besteht ein Auftragsverarbeitungsvertrag nach Art. 28 DSGVO (Version 1.2, ausgefertigt am 11.09.2026, Kundennummer K0702165720). Die Verarbeitung findet danach ausschließlich in der EU statt; der Auftragnehmer nutzt ausschließlich Serverstandorte in Deutschland
- Hetzner lässt die eigenen technischen und organisatorischen Maßnahmen mindestens jährlich durch eine unabhängige Stelle prüfen; die Ergebnisse stellt Hetzner kostenfrei bereit

Diese Maßnahmen beschreiben den Stand vom 11. September 2026. Sie werden bei Änderungen der Infrastruktur fortgeschrieben; die jeweils gültige Fassung ist unter <https://avv.ehrlich.media> abrufbar.