Technische und organisatorische Massnahmen

gemaess Art. 32 DSGVO

Julian Mueller - DeSourCeDev (jugendcampplaner.de)
Stand: 05.10.2026

Diese Übersicht fasst die tatsächlich umgesetzten technischen und organisatorischen Maßnahmen (TOM) gemäß Art. 32 DSGVO zusammen. Sie entspricht Paragraf 8 des Auftragsverarbeitungsvertrages (öffentlich einsehbar unter /avv-muster).

Vertraulichkeit

Verschlüsselung sensibler Felder

Personenbezogene Daten in den Kategorien Adress-, Gesundheits- und Krisendaten werden mit AES-256-GCM verschlüsselt gespeichert. Der Schlüssel liegt ausschließlich in der Serverkonfiguration, nicht im Quellcode.

Rollenbasierte Zugriffskontrolle

Zugriff auf personenbezogene Daten ist auf die jeweils zugehörige Organisation begrenzt; jede Aktion durchläuft eine eigene Berechtigungsprüfung.

Authentifizierung und Sitzungen

Passwort-Hashing, ein optionaler zweiter Faktor, serverseitig verwaltete Sitzungen und ein systemweiter Schutz gegen Cross-Site-Request-Forgery.

Verwahrung von Zugangsdaten

Die Kennwörter für den Mailausgang und das Postfach sowie das Erneuerungsmerkmal der Mollie-Autorisierung des Verantwortlichen werden verschlüsselt in der Datenbank gespeichert; der Schlüssel liegt ausschließlich in der Serverkonfiguration. Der kurzlebige Zugriffsschlüssel von Mollie wird nur im Arbeitsspeicher gehalten. Keines dieser Merkmale wird in Auftragsargumenten der Warteschlange oder in Protokolldateien abgelegt. Trennt der Verantwortliche die Mollie-Verbindung, wird das Erneuerungsmerkmal gelöscht und, soweit Mollie erreichbar ist, bei Mollie widerrufen.

Integrität

Unveränderlicher Protokolltrail

Sicherheitsrelevante Vorgänge werden in einem Protokoll festgehalten, das nach dem Speichern nur noch lesbar ist; ein Löschversuch schlägt technisch fehl.

Weisungsbindung

Die Verarbeitung erfolgt ausschließlich auf dokumentierte Weisung des Verantwortlichen, entsprechend dem Auftragsverarbeitungsvertrag.

Verfügbarkeit

Sicherungskonzept

Ein Sicherungskonzept mit Zeitpunkt-Wiederherstellung und verschlüsselter Ablage auf getrenntem Speicher, mit regelmäßigen Wiederherstellungsproben.

Hosting-Standort

Hosting in einem Rechenzentrum in Deutschland innerhalb der Europäischen Union. Eine Übermittlung personenbezogener Daten in Drittländer findet ausschließlich im Rahmen der Bot-Prüfung durch Cloudflare (Dienst Turnstile) statt: übermittelt werden die IP-Adresse sowie technische Angaben zu Browser, Gerät und Verbindung, kein Formularinhalt. Grundlage ist der Angemessenheitsbeschluss der Europäischen Kommission zum EU-US Data Privacy Framework. Im Übrigen finden keine Datentransfers in Drittländer statt.

Biometrische Daten

Plattformweiter Schalter

Die Gesichtserkennung ist derzeit plattformweit deaktiviert. Sie lässt sich nur über die Serverkonfiguration der Plattform einschalten; solange sie ausgeschaltet ist, werden keine biometrischen Merkmale verarbeitet. Die folgenden Maßnahmen beschreiben den Ablauf für den Fall, dass sie eingeschaltet wird.

Einmalige Verarbeitung je Lauf

Biometrische Merkmale werden nur im Rahmen eines einzelnen Erkennungslaufs verarbeitet und danach sofort gelöscht; eine dauerhafte Speicherung findet nicht statt.

Mehrfaches Überschreiben

Beim Löschen wird nach BSI-Empfehlung mehrfach überschrieben, um eine Wiederherstellung auszuschließen.

Technische Isolation

Der Gesichtserkennungsdienst ist ausschließlich lokal erreichbar; externer Netzwerkzugriff ist durch Firewall-Regeln gesperrt.

Belastbarkeit

Fehlerprotokollierung und Überwachung

Fehler werden serverseitig protokolliert; Systemzustand und Sicherungsstand werden regelmäßig geprüft.

Regelmäßige Überprüfung

Die Maßnahmen werden regelmäßig überprüft und bei Bedarf angepasst (Art. 32 Abs. 1 lit. d DSGVO).

Diese Anlage entspricht Paragraf 8 des Auftragsverarbeitungsvertrages; der vollstaendige Vertragstext ist unter /avv-muster oeffentlich einsehbar.