TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

TOM

nach Art. 32 DSGVO

Gridout [Rechtsform ergänzen] · Auftragnehmer im Sinne des Art. 28 DSGVO · Fassung vom [Datum]

Dieses Dokument beschreibt die von Gridout getroffenen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten nach Art. 32 DSGVO. Es ist Bestandteil bzw. Anlage des mit dem Auftraggeber geschlossenen Vertrages zur Auftragsverarbeitung und wird für das konkrete Projekt um die gewählte Hosting-Variante konkretisiert.

Projekt	[Projektbezeichnung]
Auftraggeber	[Firma]
Hosting-Variante	[verwaltete Cloud (Azure/AWS, Frankfurt am Main) / verwaltet bei Strato (Deutschland) / Betrieb beim Auftraggeber]

1. Vertraulichkeit

Zutrittskontrolle — Verhinderung des unbefugten physischen Zutritts zu Datenverarbeitungsanlagen

Maßnahme	Umsetzung bei Gridout
Rechenzentrum	Betrieb ausschließlich in Rechenzentren mit anerkannter Zertifizierung (ISO/IEC 27001); bei den Cloud-Anbietern zusätzlich Testate nach dem BSI-Kriterienkatalog C5. Der physische Zutrittsschutz obliegt dem jeweiligen Rechenzentrumsbetreiber.
Eigene Arbeitsräume	[Zutrittsregelung zu Räumen mit Zugriff auf Kunden- und Zugangsdaten ergänzen — z. B. abschließbare Räume, Bildschirmsperre bei Abwesenheit]
Betrieb beim Auftraggeber	Liegt in der Verantwortung des Auftraggebers als Betreiber der Infrastruktur.

Zugangskontrolle — Verhinderung der unbefugten Nutzung von Datenverarbeitungssystemen

Maßnahme	Umsetzung bei Gridout
Authentifizierung	Persönliche, nicht geteilte Zugänge für Server- und Datenbankadministration; [Passwortrichtlinie und Zwei-Faktor-Authentifizierung ergänzen, sofern eingerichtet]
Verschlüsselte Verbindungen	Administrativer Zugriff ausschließlich über verschlüsselte Verbindungen (SSH/HTTPS), kein Zugriff im Klartext
Sperrung nicht benötigter Zugänge	Regelmäßige Überprüfung und Deaktivierung nicht mehr benötigter Zugänge, insbesondere bei Projektende

Zugriffskontrolle — Berechtigte greifen nur auf die ihnen zugewiesenen Daten zu

Maßnahme	Umsetzung bei Gridout
Rollen- und Rechtekonzept	Jede Anwendung erhält ein individuelles Rollen- und Rechtekonzept; Nutzer sehen und bearbeiten nur die Daten und Funktionen, für die sie berechtigt sind
Datenbankzugriff	Zugriff auf die Datenbank ausschließlich über die Anwendung bzw. über gesondert abgesicherte administrative Zugänge; Verschlüsselung der Datenbank im Ruhezustand
Protokollierung	[Umfang der Protokollierung von Zugriffen ergänzen, sofern projektspezifisch vereinbart]

Trennungskontrolle — getrennte Verarbeitung von Daten unterschiedlicher Auftraggeber und Zwecke

Maßnahme	Umsetzung bei Gridout
Mandantentrennung	Jeder Auftraggeber erhält eine eigene, logisch getrennte Datenbank bzw. ein eigenes Datenbankschema; keine Vermischung mit Daten anderer Kunden
Trennung von Umgebungen	Trennung von Entwicklungs-, Test- und Produktivumgebung, soweit projektspezifisch vorgesehen
Pseudonymisierung	Wo möglich Einsatz pseudonymer Kennungen statt Klardaten — etwa eine tagesrotierende Prüfsumme statt der IP-Adresse bei der eigenen, cookielosen Reichweitenmessung sowie bei der Missbrauchserkennung von Formularen

2. Integrität

Weitergabekontrolle — Schutz bei Übertragung und Speicherung

Maßnahme	Umsetzung bei Gridout
Verschlüsselte Übertragung	Sämtliche Übertragung personenbezogener Daten erfolgt ausschließlich TLS-verschlüsselt (HTTPS)
Keine Weitergabe an Dritte	Eine Weitergabe erfolgt ausschließlich im Rahmen zulässiger Unterauftragsverarbeitung nach dem Vertrag zur Auftragsverarbeitung oder auf ausdrückliche Weisung des Auftraggebers
Datenträgerentsorgung	[Verfahren zur sicheren Löschung und Entsorgung von Datenträgern ergänzen, sofern eigene Hardware betroffen ist]

Eingabekontrolle — Nachvollziehbarkeit von Eingabe, Änderung und Löschung

Maßnahme	Umsetzung bei Gridout
Schutz vor Manipulation	Durchgängige Verwendung parametrisierter Datenbankabfragen zum Schutz vor SQL-Injection; Schutzmaßnahmen gegen Cross-Site-Scripting und automatisierte Missbrauchsversuche, unter anderem durch Honeypot-Felder und Begrenzung der Anfragerate
Nachvollziehbarkeit	[Protokollierung von Erstellung, Änderung und Löschung fachlicher Datensätze projektspezifisch ergänzen, z. B. über Zeitstempel- und Bearbeiterfelder]

3. Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle — Schutz vor zufälliger Zerstörung oder Verlust

Maßnahme	Umsetzung bei Gridout
Datensicherung	[Frequenz und Aufbewahrungsdauer der Datensicherungen projektspezifisch ergänzen — z. B. täglich, Aufbewahrung 30 Tage]
Redundanz	Bei den Cloud-Varianten profitiert die Anwendung von der Verfügbarkeitsarchitektur des jeweiligen Anbieters; bei Strato und beim Betrieb vor Ort [projektspezifische Maßnahmen ergänzen]

Maßnahme	Umsetzung bei Gridout
Schutz vor Angriffen	Maßnahmen gegen verbreitete Angriffsmuster wie SQL-Injection, Cross-Site-Scripting und Brute-Force-Versuche als Bestandteil des Front-End-Standards

Rasche Wiederherstellbarkeit nach Art. 32 Abs. 1 lit. c DSGVO

Maßnahme	Umsetzung bei Gridout
Wiederherstellungsverfahren	[Getestetes Verfahren zur Wiederherstellung aus Datensicherungen sowie regelmäßige Testintervalle ergänzen]

4. Verfahren zur regelmäßigen Überprüfung und Bewertung

Maßnahme	Umsetzung bei Gridout
Auftragskontrolle	Verarbeitung personenbezogener Daten ausschließlich auf dokumentierte Weisung des Auftraggebers; Unterauftragsverarbeiter werden vor Beauftragung offengelegt und nur mit Zustimmung des Auftraggebers eingesetzt
Datenschutz-Management	Internes Datenschutz-Handbuch mit Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DSGVO, Löschkonzept mit festen Fristen sowie einer Checkliste vor Aufnahme neuer Kundenprojekte
Vorfallbearbeitung	Dokumentierter Ablauf zur Erkennung, Bewertung und Meldung von Datenschutzvorfällen samt Vorfallsvorlage, um die Meldefristen nach Art. 33 DSGVO einhalten zu können
Betroffenenanfragen	Festgelegtes internes Verfahren zur Weiterleitung und Unterstützung bei Anfragen Betroffener an den Auftraggeber als Verantwortlichen
Datenschutzfreundliche Voreinstellungen	Privacy by Design und by Default als Entwicklungsgrundsatz — unter anderem eigene, cookielose Reichweitenmessung ohne dauerhafte Speicherung der IP-Adresse; bei der Tabellen-Diagnose verlässt die geprüfte Datei das Gerät des Nutzers nicht
Regelmäßige Überprüfung	[Turnus für die Aktualisierung dieses Dokuments ergänzen — z. B. jährlich sowie anlassbezogen bei wesentlichen Änderungen der Infrastruktur]

Hinweis: Dieses Dokument konkretisiert die technischen und organisatorischen Maßnahmen aus dem Vertrag zur Auftragsverarbeitung für die externe Verwendung, etwa zur Beantwortung von Sicherheitsfragebogen. Farblich hervorgehobene Textstellen in eckigen Klammern sind vor Verwendung auszufüllen und mit dem Wortlaut der zugehörigen AVV-Anlage abzugleichen.