Auftragsverarbeitungsvertrag (AVV) nach Art. 28 DSGVO

Gültig ab: 08. September 2026 | Version 1.0

zwischen dem Kunden / Maklerbetrieb (nachfolgend „Verantwortlicher“)
und
DGITel Solutions, Inhaber Daniel Göb, Max-Reger-Straße 6, 97456 Dittelbrunn (nachfolgend „Auftragsverarbeiter“)

§ 1 Gegenstand, Zweck und Dauer

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen die mandantenfähige Software-as-a-Service „DGITel Energie“ bereit. (2) Gegenstand, Art und Zweck der Verarbeitung sowie die Kategorien betroffener Personen und Datenkategorien ergeben sich aus Anlage 1 zu diesem Vertrag. (3) Die Laufzeit dieses Vertrages richtet sich nach der Laufzeit des Hauptvertrages über die Nutzung von DGITel Energie.

§ 2 Weisungsbefugnis

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen. Die vertraglich vereinbarte Bereitstellung der Software stellt die grundlegende Weisung dar. (2) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen die DSGVO oder andere Datenschutzbestimmungen verstößt.

§ 3 Vertraulichkeit und Supportzugriff

(1) Der Auftragsverarbeiter verpflichtet alle mit der Verarbeitung betrauten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit. (2) Administrativer Supportzugriff: Ein Zugriff auf Mandantendaten durch den Auftragsverarbeiter (über den Support-Account `daniel@dgitel.net`) erfolgt ausschließlich auf ausdrückliche Anforderung des Verantwortlichen, zur Störungsbeseitigung oder notwendigen Wartung. Der Support-Account wird dabei sichtbar als Mitglied in die Kundenorganisation eingebunden und nach Abschluss der Arbeiten wieder entfernt. Ein verdeckter Zugriff findet nicht statt.

§ 4 Technische und organisatorische Maßnahmen (TOMs)

(1) Der Auftragsverarbeiter trifft alle erforderlichen Maßnahmen nach Art. 32 DSGVO. Die konkreten Maßnahmen ergeben sich aus Anlage 2. (2) Der Auftragsverarbeiter behält sich vor, Sicherheitsmaßnahmen an den technischen Fortschritt anzupassen, sofern das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

§ 5 Unterauftragsverarbeiter

(1) Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine Genehmigung zur Einbindung der in Anlage 3 genannten Unterauftragsverarbeiter. (2) Der Auftragsverarbeiter informiert den Verantwortlichen mindestens 14 Tage vor der Einbindung oder Ersetzung eines Unterauftragsverarbeiters in Textform. Der Verantwortliche hat das Recht, aus wichtigem datenschutzrechtlichem Grund innerhalb dieser Frist zu widersprechen.

§ 6 Unterstützung, Vorfälle und Kontrollen

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung von Betroffenenrechten und gesetzlichen Pflichten nach Art. 32–36 DSGVO im zumutbaren Umfang. (2) Der Auftragsverarbeiter meldet dem Verantwortlichen Verletzungen des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von 48 Stunden nach Bekanntwerden. (3) Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung. Er ermöglicht und unterstützt angemessene Überprüfungen (Audits) durch den Verantwortlichen oder einen von diesem beauftragten Prüfer unter Wahrung von Betriebsgeheimnissen und nach angemessener Vorankündigung oder erbringt den Nachweis durch Vorlage aktueller Testate und Zertifizierungen.

§ 7 Beendigung und Löschung

Nach Beendigung des Hauptvertrages löscht der Auftragsverarbeiter alle im Auftrag verarbeiteten Daten innerhalb von 30 Tagen, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen. Verschlüsselte Backup-Kopien werden im Rahmen des 90-tägigen Backup-Zyklus rollierend überschrieben.

Anlage 1 – Beschreibung der Verarbeitungstätigkeit

- Gegenstand & Zweck: Bereitstellung einer B2B-SaaS-Plattform zur Verwaltung von Energie-Kunden, Zählpunkten, Aufträgen, Dokumenten und Provisionsabrechnungen durch Maklerbetriebe.

- Betroffene Personen: Endkunden und Interessenten des Maklers, dessen Ansprechpartner, Makler-Mitarbeiter und Untervermittler.
- Datenkategorien: Stammdaten (Name, Anschrift), Kontaktdaten (Telefon, E-Mail), Zählpunkt- und Lieferdaten (Zählernummer, Marktlokation, Vorversorger, Verbrauch), Bankdaten (IBAN, BIC, Kontoinhaber für Lastschriftmandate), Vertragsdokumente, Abrechnungs- und Provisionsdaten.

Anlage 2 zum AVV: Technische und organisatorische Maßnahmen (TOMs)

Stand: 08. September 2026 | Version 1.0

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

- Zutrittskontrolle: Physische Serverinfrastruktur wird in ISO-27001-zertifizierten Rechenzentren (Hetzner Online GmbH Falkenstein/Nürnberg sowie AWS Europe für Supabase/SES) mit elektronischen Schließsystemen und 24/7-Kameraüberwachung betrieben.
- Zugangskontrolle: Authentifizierung an DGITel Energie über Supabase Auth mit modernen Hash-Verfahren. Erzwingung sicherer Passwörter. Administrativer Zugriff auf Server und Datenbanken ist durch Multi-Faktor-Authentifizierung (2FA) und SSH-Key-Verfahren geschützt.
- Zugriffskontrolle & Mandantentrennung: Strenge logische Trennung aller Kundendatenbanken durch Row-Level Security (RLS) auf PostgreSQL-Ebene. Jeder Datenbankabruf wird isoliert auf Organisationsebene autorisiert. Supportzugriff erfolgt transparent und sichtbar im Dashboard des Kunden.
- Dateitrennung: Uploads und generierte Dokumente werden in separaten Storage-Buckets mit mandantenbezogenen Pfadpräfixen und Zugriffstoken abgelegt.
- Geheimnisschutz: Sensible Daten wie organisations-eigene SMTP-Passwörter werden serverseitig in verschlüsselten Vaults gespeichert und niemals im Browser-Client offengelegt.

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

- Verschlüsselung der Übertragung: Durchgängige TLS-1.3-/TLS-1.2-Verschlüsselung für alle Webtraffic- und API-Verbindungen (HTTPS).
- Verschlüsselung im Ruhezustand (at rest): Datenbanken und Objektspeicher sind auf Speicherebene (AES-256) verschlüsselt.
- Versionskontrolle & Deployment: Datenbankmigrationen sind strikt versioniert. Test- und Stagingumgebungen sind von Produktionsdaten getrennt.

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

- Redundanz: Einsatz moderner Cloud-Infrastruktur mit automatischer Hardware-Ausfallsicherung, unterbrechungsfreier Stromversorgung (USV) und DDoS-Schutzmechanismen.

- Backups: Tägliche automatisierte Backups der PostgreSQL-Produktionsdatenbank über Databasement.
- Backup-Ziel: Verschlüsselte Übertragung und Ablage auf einer Hetzner Storage Box im Rechenzentrum Falkenstein.
- Aufbewahrung & Recovery: Aufbewahrungsdauer von 90 Tagen (rollierend). Halbjährliche dokumentierte Restore-Tests zur Verifikation der Wiederherstellbarkeit. Der private Entschlüsselungsschlüssel wird getrennt von den Backup-Zielen offline/gesichert verwahrt.

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

- Regelmäßige Sicherheits- und Schwachstellen-Updates aller Serverdienste.
- Dokumentierter Incident-Management-Prozess zur Erfassung und Behebung von Systemfehlern über das interne DGITel-Ticketsystem.

Anlage 3 zum AVV: Liste der Unterauftragsverarbeiter

Stand: 08. September 2026 | Version 1.0

Dienst / Unternehmen	Sitz / Land	Verarbeitungsort	Zweck / Funktion	Rechtsgrundlage Drittlandtransfer
Supabase Pte. Ltd.	Singapur / USA	Region Frankfurt / Irland (EU)	Bereitstellung PostgreSQL-Datenbank, Auth, Storage, Edge Functions	EU-Standardvertragskla (SCC) / DPA
Cloudflare, Inc.	USA	Globales Edge-Netzwerk	CDN, Frontend-Hosting via Cloudflare Pages; Turnstile (nur `/demo`)	Data Privacy Framewor (DPF) / EU-SCCs
Hetzner Online GmbH	Gunzenhausen, Deutschland	Rechenzentrum Falkenstein (DE)	Hosting Mailserver (Mailcow VPS) & verschlüsselte Backups (Storage Box)	Auftragsverarbeitungsv (Art. 28 DSGVO)
Amazon Web Services (AWS / SES)	Luxemburg (AWS EMEA)	EU-Region	SMTP-Relay für transaktionale E-Mails	EU-Standardvertragsklause AWS-DPA
Stripe Payments Europe, Ltd.	Irland	EU / USA	Zahlungsabwicklung und Abrechnungsstatus	Data Privacy Framewor (DPF) / EU-SCCs

Hinweis zu internen Tools: Das Support-Ticketsystem (ITFlow) wird auf eigener Infrastruktur bei DGITel Solutions betrieben und stellt keinen externen Unterauftragsverarbeiter dar.