Auftragsverarbeitungsvertrag (AVV)

Muster-Vorlage nach Art. 28 DSGVO — Michailidou Digital Services I.E.

Michailidou Digital Services I.E.

2026-05-28

Contents

ACHTUNG — MUSTER — KEINE RECHTSBERATUNG

Dieses Template ist eine Vorlage. Vor produktiver Verwendung mit B2B-Kunden ist eine anwaltliche Prüfung erforderlich. Es ersetzt keine individuelle Rechtsberatung. Die Michailidou Digital Services I.E. übernimmt keine Haftung für die Verwendung dieser Vorlage ohne anwaltlichen Review.

Auftragsverarbeitungsvertrag

zwischen

Verantwortlicher (Kunde): _____

_____

— im Folgenden „Verantwortlicher" —

und

Auftragsverarbeiter: Michailidou Digital Services I.E. Zakaria Paliashvili Street 41 0179 Tiflis, Georgien

— im Folgenden „Auftragsverarbeiter" —

EU-Vertreter (Art. 27 DSGVO): Admir Xhoxha Psaron 17 12132 Peristeri, Griechenland

Präambel

Der Verantwortliche nutzt die Plattform und Dienstleistungen des Auftragsverarbeiters gemäß dem zwischen den Parteien geschlossenen Hauptvertrag (im Folgenden „Hauptvertrag"). Im Rahmen dieser Leistungserbringung verarbeitet der Auftragsverarbeiter personenbezogene Daten im Auftrag und nach Weisung des Verantwortlichen. Dieser Auftragsverarbeitungsvertrag (im Folgenden „AVV") konkretisiert die datenschutzrechtlichen Verpflichtungen der Parteien gemäß Art. 28 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, „DSGVO") und ergänzt den Hauptvertrag um die in Art. 28 Abs. 3 DSGVO geforderten Regelungen.

Der Auftragsverarbeiter hat seinen Sitz außerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums (EU/EWR). Zur Wahrnehmung der Pflichten gemäß Art. 27 DSGVO hat der Auftragsverarbeiter den oben benannten EU-Vertreter bestellt, an den sich Aufsichtsbehörden und betroffene Personen jederzeit wenden können. Übermittlungen personenbezogener Daten in Drittländer erfolgen ausschließlich auf Grundlage der EU-Standardvertragsklauseln gemäß Durchführungsbeschluss (EU) 2021/914 sowie unter Berücksichtigung etwaig ergänzender Schutzmaßnahmen.

§ 1 Gegenstand, Dauer und Beendigung

(1) Gegenstand dieses AVV ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen zur Erfüllung der im Hauptvertrag vereinbarten Leistungen. Die nähere Beschreibung von Art und Umfang der Verarbeitung ergibt sich aus Anlage 1.

(2) Die Laufzeit dieses AVV entspricht der Laufzeit des Hauptvertrags. Eine Kündigung des Hauptvertrags umfasst zugleich die Kündigung dieses AVV. Eine isolierte Kündigung dieses AVV ist ausgeschlossen, soweit der Hauptvertrag fortbesteht.

(3) Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt. Ein wichtiger Grund liegt insbesondere vor, wenn der Auftragsverarbeiter trotz schriftlicher Abmahnung und Fristsetzung gegen wesentliche datenschutzrechtliche Pflichten verstößt.

(4) Nach Beendigung der Leistungserbringung gelten die Regelungen aus § 9 dieses AVV.

§ 2 Art und Umfang der Verarbeitung (siehe Anlage 1)

(1) Zwecke, Art, Umfang und Dauer der Verarbeitung sowie die Kategorien personenbezogener Daten und betroffener Personen ergeben sich detailliert aus Anlage 1 zu diesem AVV. Anlage 1 ist integraler Bestandteil dieses Vertrags.

(2) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der in Anlage 1 beschriebenen Verarbeitungszwecke und nach den dokumentierten Weisungen des Verantwortlichen. Eine Änderung oder Erweiterung des in Anlage 1 beschriebenen Verarbeitungsumfangs bedarf einer dokumentierten Zustimmung des Verantwortlichen in Textform.

(3) Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nicht für eigene Zwecke. Eine Verarbeitung zu eigenen Zwecken des Auftragsverarbeiters (etwa zur Produkt-Verbesserung) ist nur zulässig, soweit sie auf vollständig anonymisierten Daten ohne Personenbezug beruht.

§ 3 Weisungsrecht des Verantwortlichen

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen. Dies gilt auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation, sofern nicht eine zwingende Rechtsvorschrift, der der Auftragsverarbeiter unterliegt, eine andere Anweisung verlangt.

(2) Weisungen erfolgen grundsätzlich in Textform (E-Mail genügt). Mündliche Weisungen sind nur in begründeten Einzelfällen zulässig und müssen vom Verantwortlichen unverzüglich in Textform bestätigt werden. Die im Hauptvertrag bzw. in Anlage 1 dieses AVV festgelegten Verarbeitungsparameter gelten als anfängliche Weisungen.

(3) Ist der Auftragsverarbeiter der Auffassung, dass eine Weisung des Verantwortlichen gegen datenschutzrechtliche Bestimmungen verstößt, teilt er dies dem Verantwortlichen unverzüglich in Textform mit. Bis zu einer Klärung ist der Auftragsverarbeiter berechtigt, die Durchführung der betreffenden Weisung auszusetzen.

(4) Der Auftragsverarbeiter benennt dem Verantwortlichen eine Kontaktperson für datenschutzrechtliche Belange. Aktuelle Kontaktdaten werden in Anlage 1 ausgewiesen und im Falle einer Änderung unverzüglich aktualisiert.

§ 4 Technische und organisatorische Maßnahmen (siehe Anlage 2)

(1) Der Auftragsverarbeiter ergreift alle erforderlichen technischen und organisatorischen Maßnahmen (im Folgenden „TOMs") gemäß Art. 32 DSGVO, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die konkret implementierten TOMs ergeben sich aus Anlage 2 zu diesem AVV.

(2) Der Auftragsverarbeiter überprüft seine TOMs mindestens einmal jährlich auf Wirksamkeit und Angemessenheit. Eine Anpassung an den Stand der Technik sowie an veränderte Risikolagen erfolgt fortlaufend.

(3) Wesentliche Änderungen der TOMs, die zu einer Verringerung des Sicherheitsniveaus führen könnten, werden dem Verantwortlichen vorab mit einer Frist von mindestens 4 Wochen in Textform mitgeteilt.

(4) Auf Anfrage stellt der Auftragsverarbeiter dem Verantwortlichen geeignete Nachweise zur Verfügung, insbesondere durch Audit-Berichte, Zertifikate (ISO 27001, SOC 2 Type II) seiner Sub-Auftragsverarbeiter sowie eigene Selbstauskunfts-Dokumente.

§ 5 Unter-Auftragsverarbeiter (siehe Anlage 3)

(1) Der Verantwortliche erteilt dem Auftragsverarbeiter eine allgemeine schriftliche Genehmigung zur Beauftragung der in Anlage 3 aufgeführten Unter-Auftragsverarbeiter (im Folgenden „Sub-Prozessoren").

(2) Der Auftragsverarbeiter informiert den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung von Sub-Prozessoren mit einer Frist von mindestens 4 Wochen in Textform. Der Verantwortliche kann gegen solche Änderungen aus wichtigem Grund schriftlich Einspruch erheben. Im Falle eines berechtigten Einspruchs sind die Parteien verpflichtet, gemeinsam eine angemessene Lösung zu suchen. Kann eine Einigung nicht erzielt werden, steht beiden Parteien ein außerordentliches Kündigungsrecht hinsichtlich des betroffenen Leistungsbestandteils zu.

(3) Der Auftragsverarbeiter verpflichtet die Sub-Prozessoren vertraglich zu Datenschutzregelungen, die im Wesentlichen denen dieses AVV entsprechen und insbesondere die Anforderungen des Art. 28 DSGVO erfüllen. Erfüllt ein Sub-Prozessor seine Datenschutzpflichten nicht, haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten dieses Sub-Prozessors.

(4) Sub-Prozessoren mit Sitz außerhalb der EU/EWR werden vom Auftragsverarbeiter nur auf Grundlage geeigneter Garantien gemäß Art. 44 ff. DSGVO eingesetzt, insbesondere unter Verwendung der EU-Standardvertragsklauseln und nach Durchführung einer dokumentierten Transfer-Folgenabschätzung (TIA).

§ 6 Unterstützung bei Betroffenenrechten

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung seiner Pflicht zur Beantwortung von Anträgen betroffener Personen auf Wahrnehmung ihrer Rechte gemäß Art. 15 bis Art. 22 DSGVO.

(2) Wendet sich eine betroffene Person unmittelbar an den Auftragsverarbeiter, leitet dieser das Anliegen unverzüglich an den Verantwortlichen weiter und beantwortet die betroffene Person selbst nicht inhaltlich, sondern verweist auf die Zuständigkeit des Verantwortlichen.

(3) Die Unterstützung erfolgt innerhalb angemessener Fristen, in der Regel binnen 14 Kalendertagen ab Eingang einer entsprechenden Anforderung des Verantwortlichen. Zur Auskunfts-, Berichtigungs- und Löschungsunterstützung stellt der Auftragsverarbeiter, soweit technisch möglich, Self-Service- Funktionen über die Plattform bereit.

(4) Über die Standardunterstützung hinausgehender, gesonderter Aufwand (insbesondere bei komplexen Datenexport- oder Recherche-Anforderungen) wird nach dokumentiertem Zeitaufwand zu marktüblichen Sätzen abgerechnet, sofern dies nicht im Hauptvertrag abweichend geregelt ist.

§ 7 Mitwirkungspflichten und Audit-Rechte

(1) Der Auftragsverarbeiter weist dem Verantwortlichen auf Anfrage die Einhaltung der in diesem AVV niedergelegten Pflichten in geeigneter Weise nach. Hierzu legt der Auftragsverarbeiter dem Verantwortlichen die relevanten Nachweise (TOMs-Dokumentation, Zertifikate, Audit-Berichte seiner Sub-Prozessoren) auf Anforderung in Textform vor.

(2) Der Verantwortliche ist berechtigt, einmal pro Kalenderjahr eine Vor-Ort-Prüfung oder eine entsprechende Remote-Prüfung beim Auftragsverarbeiter durchzuführen oder durch einen unabhängigen Prüfer durchführen zu lassen. Die Ankündigung erfolgt mit einer Frist von mindestens 4 Wochen in Textform. Die Prüfung erfolgt innerhalb üblicher Geschäftszeiten und unter angemessener Berücksichtigung der Betriebsabläufe des Auftragsverarbeiters.

(3) Über die Regelprüfung gemäß Abs. 2 hinaus sind anlassbezogene Prüfungen jederzeit zulässig, sofern ein begründeter Verdacht auf einen Datenschutzverstoß oder eine wesentliche Verletzung dieses AVV vorliegt. In diesem Fall verkürzt sich die Ankündigungsfrist auf 5 Werktage.

(4) Die Kosten einer Regelprüfung trägt der Verantwortliche, einschließlich des angemessenen Aufwands des Auftragsverarbeiters. Bei anlassbezogenen Prüfungen trägt der Auftragsverarbeiter die Kosten, sofern der Verdacht nach Prüfung bestätigt wird; andernfalls trägt sie der Verantwortliche.

(5) Anstelle eigener Audits kann der Verantwortliche die Vorlage aktueller Berichte unabhängiger Prüfer (insbesondere ISO 27001-, SOC 2- oder gleichwertiger Zertifizierungen der eingesetzten Sub-Prozessoren) als Nachweis akzeptieren.

§ 8 Datenpannen-Meldung

(1) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, spätestens jedoch innerhalb von 72 Stunden nach Kenntniserlangung, über jede Verletzung des Schutzes personenbezogener Daten (Art. 33 DSGVO), die im Rahmen der für den Verantwortlichen durchgeführten Verarbeitung auftritt.

(2) Die Meldung erfolgt in Textform an die vom Verantwortlichen benannten Kontaktstellen und enthält mindestens die in Art. 33 Abs. 3 DSGVO geforderten Informationen, insbesondere:

- Beschreibung der Art der Datenschutzverletzung, soweit möglich unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und Datensätze,
- Name und Kontaktdaten der zuständigen Ansprechperson beim Auftragsverarbeiter,
- Beschreibung der wahrscheinlichen Folgen der Verletzung,
- Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung und ggf. Abmilderung möglicher nachteiliger Folgen.

(3) Sind die Informationen zum Zeitpunkt der Erstmeldung noch nicht vollständig verfügbar, erfolgt die Meldung in mehreren Etappen ohne unangemessene Verzögerung. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei dessen Meldepflichten gegenüber der Aufsichtsbehörde (Art. 33 DSGVO) sowie der Benachrichtigung betroffener Personen (Art. 34 DSGVO).

(4) Eine Kopie jeder Meldung wird parallel an den EU-Vertreter (Art. 27 DSGVO) übermittelt.

§ 9 Löschung und Rückgabe nach Vertragsende

(1) Nach Beendigung der Leistungserbringung hat der Verantwortliche das Wahlrecht, ob die personenbezogenen Daten zurückgegeben oder gelöscht werden. Die Wahl ist dem Auftragsverarbeiter spätestens innerhalb von 14 Kalendertagen nach Vertragsende in Textform mitzuteilen.

(2) Soweit der Verantwortliche keine abweichende Weisung erteilt, gilt folgender Standard-Ablauf:

- Soft-Delete der personenbezogenen Daten innerhalb von 30 Kalendertagen nach Vertragsende (Daten bleiben für Wiederherstellung markiert, aber nicht mehr operativ erreichbar),
- Hard-Delete (endgültige Löschung) innerhalb weiterer 30 Kalendertage, also spätestens 60 Kalendertage nach Vertragsende.

(3) Gesetzliche Aufbewahrungspflichten (insbesondere nach HGB § 257 und AO § 147) bleiben unberührt. Daten, die solchen Aufbewahrungspflichten unterliegen, werden vom Auftragsverarbeiter getrennt gespeichert und nach Ablauf der gesetzlichen Aufbewahrungsfrist gelöscht.

(4) Der Auftragsverarbeiter erteilt dem Verantwortlichen auf Anfrage eine schriftliche Löschbestätigung mit Angabe des Datums der Löschung und einer kurzen Beschreibung des angewandten Löschverfahrens.

§ 10 Haftung

(1) Für Schäden, die einer betroffenen Person aufgrund einer datenschutzwidrigen oder sonst rechtsverletzenden Verarbeitung im Rahmen dieses AVV entstehen, haften Verantwortlicher und Auftragsverarbeiter gemeinschaftlich gegenüber der betroffenen Person nach Art. 82 DSGVO.

(2) Im Innenverhältnis tragen die Parteien Schadensersatzleistungen nach dem jeweiligen Verschuldensanteil. Hat eine Partei einen Schaden allein zu vertreten, so steht der anderen Partei kein Regressanspruch gegen sie zu.

(3) Im Übrigen gelten für die Haftung zwischen den Parteien die im Hauptvertrag vereinbarten Haftungsregelungen sowie die §§ 280 ff. BGB. Eine Haftungsbeschränkung des Auftragsverarbeiters für Vorsatz und grobe Fahrlässigkeit sowie für die Verletzung wesentlicher Vertragspflichten ist ausgeschlossen.

§ 11 Gerichtsstand und Schlussbestimmungen

(1) Änderungen und Ergänzungen dieses AVV einschließlich der Anlagen bedürfen zu ihrer Wirksamkeit der Textform. Dies gilt auch für die Aufhebung dieses Schriftformerfordernisses.

(2) Sollten einzelne Bestimmungen dieses AVV unwirksam sein oder werden, so bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die unwirksame Bestimmung ist durch eine wirksame zu ersetzen, die dem wirtschaftlichen Zweck der unwirksamen Bestimmung am nächsten kommt.

(3) Für Streitigkeiten aus oder im Zusammenhang mit diesem AVV ist das Gericht am Sitz des Verantwortlichen zuständig, soweit dies einen Gerichtsstand innerhalb der EU/EWR begründet. Für Streitigkeiten mit georgischem Bezug gilt subsidiär der Gerichtsstand Tiflis, Georgien.

(4) Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts. Zwingende Vorschriften des am Sitz des Verantwortlichen geltenden Datenschutzrechts bleiben unberührt.

§ 12 Unterschriften

Für den Verantwortlichen:

Ort, Datum: _____

Name in Druckbuchstaben: _____

Funktion: _____

Unterschrift: _____

Für den Auftragsverarbeiter (Michailidou Digital Services I.E.):

Ort, Datum: _____

Name in Druckbuchstaben: Alexia Michailidou

Funktion: Inhaberin

Unterschrift: _____

Anlage 1 — Beschreibung der Verarbeitung

Zwecke der Verarbeitung

Bereitstellung der MDS-Plattform für autonome Performance-Marketing-Workflows. Die Plattform unterstützt den Verantwortlichen insbesondere bei:

- Strategie-Generierung (KI-gestützte Erstellung von Kampagnen-Strategien)
- Creative-Produktion (KI-gestützte Erstellung von Texten, Bildern und Videos)
- Ads-Push (Übermittlung von Kampagnen-Inhalten an Google Ads, Meta Ads, LinkedIn Ads und TikTok Ads via API)
- Performance-Reporting (Aggregation und Auswertung von Plattform-Performance-Daten)
- Workflow-Orchestrierung (autonomes Pipeline-Management mit Human-in-the-Loop-Approval)

Betroffene Personenkreise

- Mitarbeiter des Verantwortlichen (Account-Nutzer der Plattform)
- Kontaktpersonen des Verantwortlichen (z. B. interne Approver)
- Ggf. Endkunden bzw. Zielgruppen-Audiences des Verantwortlichen, soweit personenbezogene Daten (z. B. Custom-Audiences, Customer-Match-Listen) vom Verantwortlichen aktiv hochgeladen werden

Kategorien personenbezogener Daten

- Account-Stammdaten (Name, E-Mail-Adresse, Rolle, Unternehmen)
- Authentifizierungs-Daten (Magic-Link-Tokens, Session-Cookies)
- Marketing-Briefings und Strategie-Eingaben (textuelle Inhalte mit ggf. enthaltenen Personenbezügen)
- Custom-Audiences (gehashte E-Mail-Adressen, Telefonnummern, sofern vom Verantwortlichen hochgeladen)
- Performance-Reportings (pseudonymisierte Klick-/Conversion-Daten der Werbe-Plattformen)
- Sub-Auftrag-Inhalte (KI-generierte Texte/Bilder/Videos, soweit Personenbezüge enthalten)
- Audit-Logs (Nutzer-ID, Zeitstempel, durchgeführte Aktion)

Verarbeitungsarten

- Speicherung in der Datenbank (Supabase, EU-Region Frankfurt)
- Speicherung von Medien-Assets in Object Storage (Hetzner, Deutschland)
- Auswertung und Aggregation für Reporting
- Übermittlung an Werbe-Plattformen via API (Google, Meta, LinkedIn, TikTok)
- KI-gestützte Inhaltsverarbeitung (Anthropic Claude, EU-Region wo verfügbar)
- E-Mail-Versand für transaktionale Benachrichtigungen (Resend, EU-Region)

Dauer der Verarbeitung

Die Verarbeitung erfolgt für die Laufzeit des Hauptvertrags zuzüglich der in § 9 dieses AVV vereinbarten Löschfristen. Aufbewahrungspflichtige Daten werden gemäß den jeweiligen gesetzlichen Vorgaben (insbesondere HGB § 257, AO § 147) aufbewahrt.

Kontaktperson für Datenschutz beim Auftragsverarbeiter

Alexia Michailidou E-Mail: michailidou.services@gmail.com

Anlage 2 — Technische und organisatorische Maßnahmen (TOMs)

Stand: 2026-05-28

1. Zutrittskontrolle (physisch)

- Sämtliche Datenverarbeitung erfolgt in Provider-Rechenzentren mit Zertifizierungen nach ISO 27001 und SOC 2 Type II (Vercel, Supabase, Anthropic, Hetzner, Fly.io). Physische Zutrittskontrolle wird durch die jeweiligen Rechenzentrums-Betreiber sichergestellt.
- Der Auftragsverarbeiter unterhält keine eigenen Räumlichkeiten mit produktiven Datenträgern. Mitarbeiter-Endgeräte werden im Home-Office-Setup mit verschlüsselten Festplatten betrieben.
- Backup-Datenträger werden ausschließlich in den Rechenzentren der Sub-Prozessoren vorgehalten; physische Übergabe von Datenträgern an Dritte erfolgt nicht.

2. Zugangskontrolle (Authentifizierung)

- Endnutzer-Authentifizierung erfolgt passwortlos über Magic-Link via Supabase Auth. Magic-Link-Tokens haben eine Lebensdauer von maximal 15 Minuten und sind Single-Use.
- Administrative Zugänge zu Vercel, Supabase und Fly.io sind mit Multi-Faktor-Authentifizierung (MFA) abgesichert. Wo verfügbar wird Single-Sign-On (SSO) genutzt.
- Service-Account-Credentials (API-Keys, Refresh-Tokens) werden regelmäßig rotiert und ausschließlich in Provider-Secret-Stores (Vercel Environment Variables, Supabase Secrets, Fly Secrets) abgelegt — niemals im Quellcode-Repository.

3. Zugriffskontrolle (Rollen und Berechtigungen)

- Alle Customer-Tabellen in der Datenbank sind durch Row-Level-Security (RLS) auf Postgres-Ebene abgesichert. Zugriffe sind ausschließlich tenant-isoliert möglich.
- Service-Accounts werden nach dem Least-Privilege-Prinzip mit minimal erforderlichen Scopes ausgestattet (z. B. Google Ads-Scope ohne Billing-Zugriff).
- Administrative Aktionen (z. B. Customer-Provisioning, manuelle Daten-Eingriffe) werden in einem Audit-Log mit Nutzer-ID, Zeitstempel und Aktion festgehalten.
- Mitarbeiter-Zugriffe auf produktive Daten werden auf das notwendige Minimum beschränkt und sind nachvollziehbar protokolliert.

4. Weitergabekontrolle

- Sämtliche Verbindungen (HTTPS, Datenbank-Connections, API-Calls zu Sub-Prozessoren und Werbe-Plattformen) erfolgen TLS-1.3-verschlüsselt.
- Verträge mit Sub-Prozessoren außerhalb EU/EWR enthalten EU-Standardvertragsklauseln gemäß Durchführungsbeschluss (EU) 2021/914 sowie ergänzende Schutzmaßnahmen wie Transfer- Folgenabschätzungen (TIA).
- Daten-Exporte für den Verantwortlichen werden verschlüsselt (AES-256) erzeugt und über zeitlich begrenzte, signierte URLs bereitgestellt.

5. Eingabekontrolle

- Datenbank-Migrationen sind versioniert und über die Git-History vollständig auditierbar (Migration-Files in `supabase/migrations/`).

- Eingehende API-Requests werden mit Nutzer-ID, Endpoint, Status-Code und Zeitstempel protokolliert (Vercel + Supabase Logs).
- Die Nachvollziehbarkeit, wer welche personenbezogenen Daten eingegeben, geändert oder gelöscht hat, wird über das Audit-Log und die DB-internen Trigger sichergestellt.

6. Verfügbarkeitskontrolle

- Tägliche Datenbank-Backups via Supabase Point-in-Time-Recovery (PITR) mit einem 7-Tage-Wiederherstellungsfenster.
- Application-Hosting (Vercel) mit Multi-Region-Failover und automatischer DDoS-Mitigation.
- Monitoring und Alerting via Vercel Observability und Supabase Logs; kritische Schwellwerte (Error-Rate, Latenz, DB-Health) führen zu automatisierten Benachrichtigungen.
- Notfall-Wiederherstellungsplan (Disaster-Recovery-Plan) ist dokumentiert.

7. Trennungskontrolle

- Multi-Tenant-Datenbank-Schema mit RLS-basierter Tenant-Isolation: Daten verschiedener Customer können logisch nicht miteinander vermengt werden.
- Logische Trennung von Customer-Workspaces über `customer_id` als Foreign-Key auf allen relevanten Tabellen.
- Separate Service-Accounts pro Customer für die Anbindung an Werbe-Plattformen (Google Ads, Meta, LinkedIn, TikTok) — kein Cross-Customer-Datenfluss möglich.

8. Pseudonymisierung und Verschlüsselung

- At-Rest-Verschlüsselung auf Datenbank-Ebene (Supabase Postgres mit transparenter Festplatten-Verschlüsselung).
- Pseudonymisierte Customer-IDs in LLM-Prompts wo möglich; Klartext-Personenbezüge werden vor Übergabe an KI-Modelle so weit wie möglich entfernt oder durch Platzhalter ersetzt.
- Verschlüsselte Backups (Supabase PITR mit Provider-seitiger Verschlüsselung).
- Custom-Audience-Daten werden vor Upload zu Werbe-Plattformen gemäß den jeweiligen Plattform-Vorgaben (SHA-256) gehasht.

9. Wiederherstellbarkeit

- Disaster-Recovery-Test wird mindestens einmal jährlich durchgeführt und dokumentiert.
- Recovery Point Objective (RPO): maximal 24 Stunden Datenverlust im Worst-Case-Szenario.
- Recovery Time Objective (RTO): maximal 4 Stunden für Application-Restore, maximal weitere 8 Stunden für Daten-Restore aus PITR.
- Backup-Restore-Verfahren sind dokumentiert und werden im Rahmen der Disaster-Recovery-Tests verifiziert.

10. Verfahren zur regelmäßigen Überprüfung

- Quartalsweises internes Review der TOMs durch den Auftragsverarbeiter, dokumentiert in einem internen TOM-Review-Protokoll.
- Jährlicher externer Penetrationstest für Customers ab Tier-B (Enterprise-Tier), durchgeführt durch einen unabhängigen Sicherheits-Dienstleister.
- Aktualisierungspflicht bei wesentlichen Stand-der-Technik- Änderungen sowie nach jedem dokumentierten Sicherheitsvorfall.

- Datenschutz-Folgenabschätzungen (DSFA) werden bei wesentlichen Verarbeitungs-Änderungen durchgeführt und dem Verantwortlichen auf Anfrage zur Verfügung gestellt.

Anlage 3 — Sub-Auftragsverarbeiter

Stand: 2026-05-28

#	Anbieter	Sitz	Zweck	Datenresidenz	Rechtsgrundlage
1	Vercel Inc.	Covina, CA, USA	Application-Hosting & CDN	EU (fra1, Frankfurt)	DPF + SCC (Vercel DPA)
2	Supabase Inc.	Singapur / USA	Datenbank & Authen-tifizierung	EU (eu-central-1, Frankfurt)	SCC (Supabase DPA)
3	Anthropic, PBC	San Francisco, USA	KI-Inferenz (Claude-Modelle)	EU-Region wo verfügbar, US-Fallback	SCC (Anthropic Enterprise DPA)
4	Hetzner Online GmbH	Gunzenhausen, Deutschland	File-Storage (Object Storage)	DE (FSN1/NBG1, Falken-stein/Nürnberg)	DSGVO direkt (DE-Anbieter)
5	Resend Inc.	Wilmington, DE, USA	Transaktionale E-Mails	EU-Region (Ireland)	SCC (Resend DPA)
6	Fly.io	Chicago, IL, USA	Worker-Compute	EU (fra-Region, Frankfurt)	SCC (Fly.io DPA)
7	Stripe Inc.	South San Francisco, CA, USA	Payment-Processing	EU + US (SCCs)	DPF + SCC (Stripe DPA)
8	Google Ireland Ltd.	Dublin, Irland	Calendar / Analytics (opt-in)	EU / USA	DPF (nur bei expliziter Einwilligung)

Anbieter-DPAs (öffentlich)

- Vercel: https://vercel.com/legal/dpa
- Supabase: https://supabase.com/legal/dpa
- Anthropic: https://www.anthropic.com/legal/dpa
- Hetzner: https://www.hetzner.com/de/rechtliches/datenschutz
- Resend: https://resend.com/legal/dpa
- Fly.io: https://fly.io/legal/dpa
- Stripe: https://stripe.com/legal/dpa
- Google Cloud: https://cloud.google.com/terms/data-processing-terms

Die Original-DPAs der Anbieter gelten als integraler Bestandteil dieses AVV. Auf Anfrage stellen wir die Versionsstände unserer akzeptierten DPAs (Datum + Hash) als Compliance-Beleg bereit.