AUFTRAGSVERARBEITUNGSVERTRAG (AVV)

gemäß Art. 28 DSGVO
EventCommand – eventcommand.de
Version 1.4 · Stand: 26. Oktober 2026

Parteien

Auftragsverarbeiter:

Ayke Bröcker – Brienzer Str. 59, 13407 Berlin

E-Mail: support [at] eventcommand [punkt] de | Tel.: +49 30 46062303

(nachfolgend: „Auftragsverarbeiter“)

Verantwortlicher:

Name / Unternehmen: _____

Adresse: _____

E-Mail: _____

Vertreten durch: _____

(nachfolgend: „Verantwortlicher“)

Die Anlagen 1 (Technische und organisatorische Maßnahmen) und 2 (Unterauftragsverarbeiter) sind Bestandteil dieses Vertrages.

1. Gegenstand, Art, Zweck und Dauer der Verarbeitung

Dieser Vertrag regelt die Rechte und Pflichten der Parteien gemäß Art. 28 DSGVO. Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag und nach dokumentierter Weisung des Verantwortlichen im Rahmen der Nutzung von EventCommand.

Merkmal	Beschreibung
Gegenstand	Bereitstellung und Betrieb der EventCommand-Plattform für Organisationen, Veranstalter und deren eingeladene Nutzer.
Art der Verarbeitung	Erheben, Erfassen, Organisation, Ordnen, Speichern, Strukturieren, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung innerhalb der Plattform, Einschränken, Löschen und Vernichten.
Zweck	Verwaltung von Veranstaltungsstrukturen, Rollen, Organigrammen, Freigaben, Ablauf- und Schichtplanung, Verfügbarkeiten, Kontakten, Funkplanung, Dokumenten, Notfall-/Vorfallprotokollen, Audit-Logs und Kalender-Abonnements.
Dauer	Laufzeit des Nutzungsverhältnisses; danach Löschung oder Rückgabe gemäß Ziff. 4.9 und den Backup-/Löschroutinen der eingesetzten Systeme.

Nicht Gegenstand dieses AVV sind Verarbeitungen, bei denen der Auftragsverarbeiter selbst Verantwortlicher ist, insbesondere eigene Vertragsverwaltung einschließlich Dokumentation

der AGB-/AVV-Annahme (Organisation, akzeptierender Nutzer, Zeitstempel, Version, IP-Adresse und User-Agent), Rechnungsstellung, allgemeine Kontoverwaltung, Marketing-Einwilligungen, Supportkommunikation und eigene Sicherheits-/Missbrauchsprävention, soweit diese nicht ausschließlich im Auftrag des Verantwortlichen erfolgen.

2. Art der personenbezogenen Daten

Datenkategorie	Konkrete Daten
Stammdaten	Name, optional Vorname, Profilname, Firma/Organisation, eventbezogene Stammdaten-Snapshots.
Kontakt- und Kommunikationsdaten	E-Mail-Adressen, optionale abweichende Kommunikations-E-Mail, Telefonnummern, Funkkanäle, Einladungsdaten, Zustellinformationen für Service-Mails.
Organisations- und Rollendaten	Organisationszugehörigkeit, Rollen, Funktionen, Berechtigungen, Organigramm, Verantwortlichkeiten, Sichtbarkeitsstufen.
Event- und Betriebsdaten	Eventname, Beschreibung, Datum, Status, Ablaufpläne, Schichten, Verfügbarkeiten, Zuordnungen, Funkplanung, Freigaben, Widerrufe, Begründungen.
Kontaktpersonen und Zusatzkontakte	Name, E-Mail, Telefon, Firma, Funktion, frei angelegte Zusatzkontakte, Notfallkontakte, Krisenstab.
Dokumenteninhalte	Hochgeladene PDF-Dokumente mit gegebenenfalls personenbezogenem Inhalt.
Notfall-/Vorfalldaten	Zeitpunkt, Ort, Status, Maßnahmen, Zuständigkeiten, Protokolleinträge und sonstige vom Verantwortlichen eingegebene Informationen.
Technische Daten	IP-Adressen, Zugriffszeitstempel, Session-/Authentifizierungsinformationen, Audit-Logs, Nutzerkennung, Aktion, Zeitpunkt, betroffene Organisation/Eventstruktur.
Kalenderdaten	Schicht-, Ablauf- und Zeitplandaten im .ics-Feed sowie Capability-Tokens.

Besondere Kategorien personenbezogener Daten gem. Art. 9 DSGVO sind nicht Standardgegenstand der Verarbeitung. Insbesondere sollen Gesundheitsdaten, Diagnosen, Verletzungsdetails, medizinische Behandlungen, Gewerkschaftszugehörigkeit, politische Meinungen oder vergleichbare sensible Daten nicht in die Plattform eingegeben werden, sofern keine gesonderte dokumentierte Weisung und keine tragfähige Rechtsgrundlage bzw. Ausnahme nach Art. 9 DSGVO vorliegt. Der Verantwortliche bleibt für die Rechtmäßigkeit solcher Eingaben verantwortlich.

3. Kreis der betroffenen Personen

- registrierte Nutzer der Organisation, insbesondere Org-Owner, Admins und Mitglieder
- Event-Mitarbeitende, Freelancer, Dienstleister und projektbezogen eingeladene Personen
- Gäste oder externe Beteiligte, die einem Event beitreten oder Stammdaten freigeben

- in der Plattform eingetragene Kontaktpersonen, Zusatzkontakte, Notfallkontakte und Krisenstab-Mitglieder
- sonstige Personen, deren Daten durch den Verantwortlichen oder berechtigte Nutzer in die Plattform eingegeben werden

4. Pflichten des Auftragsverarbeiters

4.1 Weisungsgebundenheit

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, insbesondere über die Plattformfunktionen oder per E-Mail an support [at] eventcommand [punkt] de, es sei denn, er ist durch Unionsrecht oder Recht eines Mitgliedstaats zur Verarbeitung verpflichtet. In diesem Fall informiert der Auftragsverarbeiter den Verantwortlichen vor der Verarbeitung über die rechtliche Anforderung, sofern das betreffende Recht eine solche Information nicht aus wichtigen Gründen des öffentlichen Interesses verbietet. Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, informiert er den Verantwortlichen unverzüglich.

4.2 Vertraulichkeit

Der Auftragsverarbeiter stellt sicher, dass alle zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet sind oder einer gesetzlichen Verschwiegenheitspflicht unterliegen.

4.3 Technische und organisatorische Maßnahmen

Der Auftragsverarbeiter trifft die in Anlage 1 beschriebenen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO. Er ist berechtigt, die Maßnahmen anzupassen, soweit das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen, die das Schutzniveau berühren, werden dem Verantwortlichen vorab oder unverzüglich nach Umsetzung mitgeteilt, soweit dies sicherheits- oder betriebsbedingt erforderlich ist.

4.4 Unterauftragsverarbeiter

Der Verantwortliche erteilt eine allgemeine schriftliche Genehmigung für den Einsatz der in Anlage 2 aufgeführten Unterauftragsverarbeiter. Bei der Hinzuziehung neuer oder dem Austausch bestehender Unterauftragsverarbeiter informiert der Auftragsverarbeiter den Verantwortlichen mindestens 14 Tage im Voraus per E-Mail oder über einen geeigneten elektronischen Informationsweg. Der Verantwortliche kann innerhalb von 14 Tagen aus wichtigem datenschutzrechtlichem Grund Einspruch erheben. Kann dem Einspruch nicht abgeholfen werden, kann der Verantwortliche die betroffenen Leistungen kündigen.

Der Auftragsverarbeiter stellt sicher, dass mit Unterauftragsverarbeitern Datenschutzpflichten vereinbart werden, die den Pflichten dieses Vertrages im Wesentlichen entsprechen. Der Auftragsverarbeiter bleibt gegenüber dem Verantwortlichen für die Erfüllung der Pflichten der Unterauftragsverarbeiter verantwortlich.

4.5 Unterstützung bei Betroffenenrechten

Der Auftragsverarbeiter unterstützt den Verantwortlichen nach Möglichkeit durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung von Auskunfts-, Berichtigungs-, Löschungs-, Einschränkungs-, Übertragbarkeits- und Widerspruchsansprüchen nach Art. 15 bis 22 DSGVO. Entsprechende Anfragen sind per E-Mail zu stellen. Der Auftragsverarbeiter antwortet regelmäßig innerhalb von 5 Werktagen, soweit die Anfrage nicht aufgrund Umfang, Komplexität oder Abhängigkeit von Unterauftragsverarbeitern eine längere Bearbeitung erfordert.

4.6 Meldung von Datenschutzverletzungen

Der Auftragsverarbeiter meldet Verletzungen des Schutzes personenbezogener Daten, die Daten des Verantwortlichen betreffen, unverzüglich, möglichst innerhalb von 48 Stunden nach Bekanntwerden, per E-Mail an den Verantwortlichen. Die Meldung enthält, soweit bekannt, Art der Verletzung, betroffene Datenkategorien und Personen, voraussichtliche Folgen sowie ergriffene oder geplante Abhilfemaßnahmen. Der Auftragsverarbeiter unterstützt den Verantwortlichen angemessen bei dessen Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO.

4.7 Datenschutz-Folgenabschätzung und Vorabkonsultation

Der Auftragsverarbeiter unterstützt den Verantwortlichen nach Möglichkeit bei Datenschutz-Folgenabschätzungen nach Art. 35 DSGVO und Vorabkonsultationen nach Art. 36 DSGVO durch Bereitstellung relevanter Informationen über die Verarbeitungsinfrastruktur, soweit diese dem Auftragsverarbeiter vorliegen und der Verantwortliche sie nicht selbst über die Plattform oder Anbieterinformationen erhalten kann.

4.8 Nachweis und Überprüfung

Der Auftragsverarbeiter stellt dem Verantwortlichen alle zur Nachweisführung gemäß Art. 28 Abs. 3 lit. h DSGVO erforderlichen Informationen zur Verfügung. Als Nachweis können geeignete Dokumentationen, TOM-Beschreibungen, Zertifizierungen, Auditberichte oder Sicherheitsnachweise der Unterauftragsverarbeiter bereitgestellt werden. Physische oder technische Inspektionen sind nur nach angemessener Vorlaufzeit von mindestens 30 Tagen, während üblicher Geschäftszeiten, bei Wahrung von Vertraulichkeit und ohne Beeinträchtigung von Sicherheit oder Betrieb möglich. Der Verantwortliche trägt die durch eine individuelle Prüfung entstehenden angemessenen Kosten, soweit gesetzlich zulässig.

4.9 Löschung und Rückgabe

Nach Beendigung des Nutzungsverhältnisses löscht oder gibt der Auftragsverarbeiter nach Wahl des Verantwortlichen alle personenbezogenen Daten zurück, sofern keine gesetzliche Pflicht zur Speicherung besteht. Der Verantwortliche kann bis zu 30 Tage nach Vertragsende einen Datenexport anfordern. Nach Ablauf der Karenzzeit erfolgt die Löschung der produktiven Daten nach den technisch vorgesehenen Routinen. Sicherungskopien gemäß Ziff. 4.10 enthalten die Daten noch bis zu 30 Tage nach Löschung der produktiven Daten und werden danach automatisch gelöscht; bis dahin werden sie nicht für andere Zwecke genutzt, und beim Zurückspielen einer Sicherung werden bereits gelöschte Daten erneut gelöscht. Backups der Unterauftragsverarbeiter werden nach deren jeweiligen Backup-Zyklen überschrieben oder gelöscht. Eine Löschbestätigung kann auf Anfrage ausgestellt werden.

4.10 Datensicherung

Der Auftragsverarbeiter erstellt zur Datensicherung regelmäßig Sicherungskopien der Plattformdaten. Diese werden verschlüsselt gespeichert und nach 30 Tagen gelöscht. Die Sicherungen dienen ausschließlich der Wiederherstellung nach Datenverlust; der Zugriff darauf ist auf den Auftragsverarbeiter beschränkt. Das Sicherungssystem wird vom Auftragsverarbeiter selbst betrieben.

5. Pflichten des Verantwortlichen

- Sicherstellung der Rechtmäßigkeit der Verarbeitung, insbesondere für Daten von Crew, Gästen, Freelancern, Zusatzkontakten und sonstigen Dritten.
- Erfüllung der Informationspflichten nach Art. 13 und 14 DSGVO gegenüber betroffenen Personen, soweit der Verantwortliche deren Daten in die Plattform eingibt oder durch Nutzer eingeben lässt.

- Erteilung dokumentierter, rechtmäßiger und zweckgebundener Weisungen.
- Konfiguration und Kontrolle von Rollen, Berechtigungen und Sichtbarkeiten innerhalb der Organisation.
- Prüfung, ob eine Datenschutz-Folgenabschätzung erforderlich ist.
- Keine Eingabe von Art.-9-Daten, insbesondere Gesundheitsdaten, ohne eigene tragfähige Rechtsgrundlage, Ausnahme nach Art. 9 DSGVO, Datenminimierung und gesonderte dokumentierte Weisung.
- Unverzügliche Information des Auftragsverarbeiters bei festgestellten Unregelmäßigkeiten oder Datenschutzrisiken.
- Sicherstellung, dass eigene Nutzer nur solche Daten in EventCommand verarbeiten, die für den jeweiligen Zweck erforderlich sind.

6. Drittlandtransfers

Die produktive technische Konfiguration von EventCommand ist auf EU-Regionen ausgerichtet: Vercel Functions sind auf fra1 Frankfurt/EU konfiguriert, Supabase wird in eu-central-1 Frankfurt/EU betrieben und die Resend-Versandregion ist eu-west-1 Irland. Gleichwohl sind die eingesetzten Unterauftragsverarbeiter US-Unternehmen. Zudem können Accountdaten, Service-Generated Data, Support-, Sicherheits- und Logdaten sowie E-Mail-Metadaten oder API-Records in den USA verarbeitet oder aus den USA zugänglich sein. Eine pauschale EU-only-Zusage ist daher nicht Gegenstand dieses AVV.

Anbieter	Sitz	Leistung	Transfermechanismus
Vercel Inc.	USA	Hosting, CDN, Serverless Functions, Build-Pipeline	EU-US Data Privacy Framework; ergänzend Transfermechanismen/SCC nach Vercel-DPA, soweit erforderlich.
Supabase Inc.	USA	PostgreSQL-Datenbank, Authentifizierung, Datei-Storage, Zugriffskontrolle	Standardvertragsklauseln bzw. Transfermechanismen des Supabase-DPA.
Plus Five Five, Inc. / Resend	USA	Service-Mails und optionale Marketing-/Produkt-News	EU-US Data Privacy Framework; ergänzend EU-Standardvertragsklauseln nach Resend-DPA.
Google Ireland Ltd. / Google LLC	Irland / USA	Push-Zustellung (Firebase Cloud Messaging) an Chrome und die Android-App	EU-US Data Privacy Framework; ergänzend Standardvertragsklauseln, soweit erforderlich.
Apple Distribution International Ltd. / Apple Inc.	Irland / USA	Push-Zustellung (Apple Push Notification service) an Safari (iOS/macOS) und die iOS-App	EU-US Data Privacy Framework; ergänzend Standardvertragsklauseln, soweit erforderlich.

Der Verantwortliche nimmt zur Kenntnis, dass die genannten Anbieter weitere Unterauftragsverarbeiter einsetzen können. Die jeweils aktuellen Subprozessorlisten der Anbieter sind Grundlage der Anbieter-DPA und werden in Anlage 2 referenziert.

7. Haftung

Die Parteien haften gegenüber betroffenen Personen nach den gesetzlichen Vorgaben, insbesondere Art. 82 DSGVO. Im Innenverhältnis haften die Parteien nach ihrem jeweiligen Verantwortungs- und Verursachungsbeitrag. Die Haftungsregelungen der Nutzungsbedingungen gelten ergänzend, soweit sie wirksam vereinbart sind und zwingende Datenschutzvorgaben nicht unterschreiten.

8. Laufzeit und Kündigung

Dieser Vertrag läuft parallel zum Nutzungsverhältnis zwischen den Parteien. Er endet automatisch mit vollständiger Beendigung des Nutzungsverhältnisses und Abschluss der Löschung oder Rückgabe der personenbezogenen Daten. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt, insbesondere bei schwerwiegenden oder wiederholten Verstößen gegen datenschutzrechtliche Pflichten.

9. Anwendbares Recht und Gerichtsstand

Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist Berlin, soweit gesetzlich zulässig.

10. Rangfolge

Bei Widersprüchen zwischen diesem AVV und sonstigen Vereinbarungen gehen die Regelungen dieses AVV für die Verarbeitung personenbezogener Daten im Auftrag vor. Zwingende gesetzliche Vorgaben bleiben unberührt.

11. Unterschriften / elektronische Annahme

Dieser AVV kann schriftlich, elektronisch oder durch dokumentierte Annahme im Rahmen der Plattform abgeschlossen werden. Bei elektronischer Annahme protokolliert EventCommand pro Organisation insbesondere Organisation-ID, akzeptierenden Nutzer, Zeitpunkt der Annahme, AVV-Version, AGB-Version, IP-Adresse und User-Agent.

Diese Nachweisdaten werden ausschließlich zweckgebunden zur Vertragsdokumentation, zum Nachweis der Annahme von AGB und AVV sowie zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche verarbeitet. Eine Nutzung zu Tracking-, Marketing- oder Profiling-Zwecken findet nicht statt.

Die Verarbeitung dieser Nachweisdaten erfolgt durch EventCommand als eigener Verantwortlicher und ist nicht Gegenstand der Auftragsverarbeitung nach diesem AVV. Die Aufbewahrung erfolgt für die Dauer des Vertragsverhältnisses und anschließend für gesetzliche Verjährungs- und Nachweisfristen, regelmäßig bis zum Ablauf von drei Jahren nach Ende des Jahres, in dem das Vertragsverhältnis endet. Bei laufenden Ansprüchen, Streitigkeiten oder gesetzlichen Aufbewahrungspflichten erfolgt die Speicherung entsprechend länger bis zu deren Abschluss oder Ablauf.

Ort, Datum: _____

Ayke Bröcker / EventCommand (Auftragsverarbeiter)

Name, Funktion (Verantwortlicher)

ANLAGE 1 – TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN (TOMs)

gemäß Art. 32 DSGVO | Version 1.4 · Stand: 26. Oktober 2026

1. Zutrittskontrolle

- Cloud-basierter Betrieb der Plattform über Vercel, Supabase/AWS und Resend/AWS; zusätzliche Datensicherungen auf einem vom Betreiber selbst betriebenen Speichersystem.
- Physischer Zugang zu Serverinfrastruktur wird durch die jeweiligen Rechenzentrums- und Cloudanbieter kontrolliert.
- Der Betreiber hat keinen physischen Zugang zu den Servern der Cloudanbieter. Das Speichersystem für Datensicherungen befindet sich in den Geschäftsräumen des Betreibers; Zutritt nur durch den Betreiber.

2. Zugangskontrolle

- Authentifizierung per E-Mail und Passwort über Supabase Auth.
- Passworthashing durch Supabase Auth; kein Klartextzugriff durch den Betreiber.
- Session-Management über Supabase Auth und JWT-basierte Sitzungen.
- Passwort-Reset und E-Mail-Änderungen nur über verifizierte E-Mail-Prozesse.
- Administrativer Betreiberzugriff nur für berechtigte Betreiberkonten.
- Zugangsdaten und Schlüssel (z. B. Datenbankpasswort, Storage-Schlüssel) werden ausschließlich auf dem Sicherungssystem und in einem Passwortmanager verwahrt.

3. Zugriffskontrolle

- Row Level Security (RLS) zur mandantenbezogenen Zugriffsbeschränkung auf Datenbankebene.
- Rollenbasiertes Zugriffsmodell, insbesondere Owner, Admin, Member, Viewer bzw. funktionsbezogene Event-Rollen.
- Event-Mitarbeitende und Gäste sehen nur die für sie freigegebenen Event- und Organisationsdaten.
- Zusatzkontakte können mit eingeschränkter Sichtbarkeit angelegt werden.
- Privater Storage für PDF-Dokumente; Abruf nur für berechtigte Nutzer.

4. Weitergabekontrolle

- Ausschließlich verschlüsselte Übertragung per HTTPS/TLS.
- Datenbankverbindungen und API-Zugriffe nur über abgesicherte Schnittstellen.
- Dokument-Downloads nur über signierte, zeitlich begrenzte URLs.
- Kalender-Feeds nur über nicht erratbare Capability-Tokens.
- Keine Weitergabe an Dritte außer an die in Anlage 2 genannten Unterauftragsverarbeiter oder aufgrund gesetzlicher Verpflichtung.

5. Eingabekontrolle

- Datenänderungen werden mit Nutzerkennung und Zeitstempel protokolliert, soweit technisch vorgesehen.
- Freigaben, Widerrufe, Einladungen und relevante Statusänderungen werden mit Zeitstempel gespeichert.
- Audit-Logs dokumentieren sicherheits- und nachweisrelevante Aktionen.

6. Auftragskontrolle

- Verarbeitung ausschließlich gemäß Hauptvertrag, AVV und dokumentierten Weisungen.
- Unterauftragsverarbeiter nur gemäß Anlage 2 und den Regelungen dieses AVV.
- Vertragliche Einbindung der Unterauftragsverarbeiter über DPA/AVV und geeignete Transfermechanismen.

7. Verfügbarkeitskontrolle

- Plan- und anbieterabhängige Datenbank-Backups durch Supabase.
- Nutzung hochverfügbarer Cloud-Infrastruktur und Wiederherstellungsmechanismen der Anbieter.
- Betriebliche Überwachung von Fehlern und Sicherheitsereignissen.
- Löschungen und Backup-Retention nach dokumentierten Betriebsprozessen.
- Regelmäßige Datensicherung der Plattformdaten (Nutzerkonten, Events, Rollen, Kontakte, hochgeladene Dokumente) auf einem selbst betriebenen Speichersystem; verschlüsselte Speicherung, Aufbewahrung 30 Tage, danach automatische Löschung.
- Zugriff auf das Sicherungssystem nur durch den Betreiber; Zwei-Faktor-Anmeldung, aktuell gehaltene Systemsoftware, kein Zugriff aus dem Internet (keine Portfreigabe, keine Fernzugriffsdienste).
- Restore-Test der Datensicherung quartalsweise.
- Sichere Löschung der Datenträger bei Außerbetriebnahme oder Entsorgung des Sicherungssystems; bei Verlust schützt die Verschlüsselung.

8. Trennungsgebot

- Mandantenfähige Trennung nach Organisationen.
- RLS und rollenbasierte Berechtigungen stellen sicher, dass Nutzer grundsätzlich nur Daten ihrer Organisation bzw. freigegebenen Events sehen.
- Trennung von produktiven Organisationsdaten, Authentifizierungsdaten und Datei-Storage-Berechtigungen.

9. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

- Minimierung der Datenerhebung auf für die App-Funktionen erforderliche Daten.
- Keine Analyse-/Tracking-Tools, keine Werbenetzwerke und keine Marketing-Cookies.
- Marketing-Checkbox standardmäßig leer; Marketing-Mails nur bei aktivem Opt-in oder gesetzlicher Ausnahme.
- Keine Öffnungs- oder Klicktracking-Funktionen in E-Mails.
- Kalender-Feeds enthalten keine fremden Kontaktdaten.

10. Dokumentations- und Kontrollmaßnahmen

- Interne Dokumentation der eingesetzten Dienste, Regionen, DPA/AVV und Subprozessorlisten.
- Protokollierung von AGB-/AVV-Annahmen einschließlich Organisation, Nutzer, Zeitstempel, Version, IP-Adresse und User-Agent als zweckgebundener Vertragsnachweis.
- Regelmäßige Überprüfung der Anbieterinformationen zu Regionen, DPA, Subprozessoren und Transfermechanismen.

ANLAGE 2 – UNTERAUFTRAGSVERARBEITER

gemäß Art. 28 Abs. 4 DSGVO | Version 1.4 · Stand: 26. Oktober 2026

Anbieter / Sitz	Leistung	Region / Verarbeitung	Rechtsgrundlage / Hinweise
Vercel Inc., USA	Hosting des Frontends, CDN, Serverless Functions, Build-Pipeline	Functions für EventCommand auf fra1 Frankfurt/EU konfiguriert; CDN/global verteilte Auslieferung statischer Inhalte möglich.	DPA besteht; EU-US Data Privacy Framework; ergänzend SCC/Transfermechanismen nach Vercel-DPA. Aktuelle Subprozessoren: https://security.vercel.com
Supabase Inc., USA	PostgreSQL-Datenbank, Authentifizierung, Datei-Storage (PDF), Zugriffskontrolle	Projektregion eu-central-1 Frankfurt/EU.	DPA besteht; SCC/Transfermechanismen nach Supabase-DPA. Aktuelle Subprozessoren: https://supabase.com/legal/customer-resources/subprocessor-list
Plus Five Five, Inc. / Resend 2261 Market Street #5039 San Francisco, CA 94114, USA	Versand von Service-Mails und optionalen Marketing-/Produkt-News	Versandregion eu-west-1 Irland. Accountdaten, E-Mail-Metadaten, Logs und API-Records können nach Anbieterinformation in den USA gespeichert werden. Open-/Clicktracking ist in EventCommand deaktiviert.	DPA besteht; EU-US Data Privacy Framework; EU-SCC nach Resend-DPA. Aktuelle Subprozessoren: https://resend.com/legal/subprocessors
Google Ireland Ltd., Irland / Google LLC, USA	Push-Zustellung (Firebase Cloud Messaging) an Chrome und die Android-App; verarbeitet werden Push-Token und Benachrichtigungsinhalt	Zustellung über Google-Infrastruktur; Verarbeitung auch in den USA möglich.	EU-US Data Privacy Framework; ergänzend Standardvertragsklauseln, soweit erforderlich.
Apple Distribution International Ltd., Irland / Apple Inc., USA	Push-Zustellung (Apple Push Notification service) an Safari (iOS/macOS) und die iOS-App; verarbeitet werden Push-Token und Benachrichtigungsinhalt	Zustellung über Apple-Infrastruktur; Verarbeitung auch in den USA möglich.	EU-US Data Privacy Framework; ergänzend Standardvertragsklauseln, soweit erforderlich.

Hinweis: Bei der Hinzuziehung neuer Unterauftragsverarbeiter informiert der Auftragsverarbeiter den Verantwortlichen gemäß Ziff. 4.4 mindestens 14 Tage im Voraus. Die Anbieter können ihre eigenen Subprozessorlisten aktualisieren; diese sind regelmäßig zu überprüfen. Das vom Auftragsverarbeiter selbst betriebene Sicherungssystem ist kein Unterauftragsverarbeiter. Setzt der Auftragsverarbeiter künftig einen externen Speicherdienst für Datensicherungen ein, wird dieser in diese Anlage aufgenommen und nach Ziff. 4.4 angekündigt.

Version 1.4 · Stand: 26. Oktober 2026