DATENSCHUTZERKLÄRUNG

EventCommand – eventcommand.de

Version 1.5 · Stand: 26. Oktober 2026

1. Verantwortlicher

Verantwortlicher im Sinne der Datenschutz-Grundverordnung (DSGVO) ist:

Ayke Bröcker

Brienzer Str. 59, 13407 Berlin, Deutschland

E-Mail: support [at] eventcommand [punkt] de

Telefon: **+49 30 46062303**

Web: https://eventcommand.de | App: https://app.eventcommand.de

Nachfolgend bezeichnen „wir“, „uns“ oder „Betreiber“ den vorstehenden Verantwortlichen.

2. Rollenverteilung bei der Nutzung von EventCommand

EventCommand verarbeitet personenbezogene Daten in unterschiedlichen Rollen.

Soweit wir Kontodaten registrierter Nutzer, Vertrags- und Rechnungsdaten, technische Betriebs- und Sicherheitsdaten, Supportvorgänge sowie Marketing-Einwilligungen verarbeiten, handeln wir als Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO.

Soweit Organisationen, Veranstalter oder Org-Owner innerhalb von EventCommand Daten zu Events, Rollen, Crew-Mitgliedern, Gästen, Freelancern, Kontakten, Schichten, Verfügbarkeiten, Freigaben, Dokumenten, Notfall-/Vorfallprotokollen oder Audit-Logs verwalten, verarbeiten wir diese Daten grundsätzlich im Auftrag des jeweiligen Organisationskunden. Verantwortlich für Zwecke, Rechtsgrundlagen, Datenminimierung und Information der betroffenen Personen ist in diesen Fällen der jeweilige Organisationskunde. Die Verarbeitung durch EventCommand erfolgt auf Grundlage eines Auftragsverarbeitungsvertrags nach Art. 28 DSGVO.

Betroffenenanfragen, die sich auf Daten beziehen, die wir im Auftrag eines Organisationskunden verarbeiten, leiten wir an den jeweiligen Organisationskunden weiter oder bearbeiten sie nach dessen dokumentierter Weisung.

3. Gegenstand und Zweck des Dienstes

EventCommand ist eine mobile-first Web-App für Veranstaltungsprofis. Die Plattform dient der Verwaltung von Events, Rollen und Organigrammen, Freigaben, Notfall- und Vorfalldokumentation, Ablauf- und Schichtplanung, Kontakten, Funkplanung, Dokumenten und Kalender-Abonnements. Der Dienst richtet sich an gewerbliche Nutzer und Organisationen im B2B-Kontext. Eingeladene Gäste, Freelancer und Crew-Mitglieder können Funktionen nutzen, soweit sie von einem Organisationskunden eingeladen werden.

In der App findet keine Zahlungsabwicklung statt. Upgrades, Vertragsänderungen und Abrechnung erfolgen außerhalb der App persönlich oder per E-Mail.

4. Rechtsgrundlagen

Wir stützen die Verarbeitung personenbezogener Daten, soweit wir selbst Verantwortlicher sind, insbesondere auf folgende Rechtsgrundlagen:

- Art. 6 Abs. 1 lit. a DSGVO – Einwilligung, insbesondere für optionale Marketing-/Produkt-News.
- Art. 6 Abs. 1 lit. b DSGVO – Vertragserfüllung oder vorvertragliche Maßnahmen, insbesondere Nutzerkonto, Bereitstellung der App-Funktionen und Abrechnung.
- Art. 6 Abs. 1 lit. c DSGVO – rechtliche Verpflichtungen, insbesondere steuer- und handelsrechtliche Aufbewahrungspflichten.
- Art. 6 Abs. 1 lit. f DSGVO – berechtigte Interessen, insbesondere IT-Sicherheit, Missbrauchsprävention, Nachweis von Handlungen, Support, Fehleranalyse und betriebliche Stabilität.

Soweit wir personenbezogene Daten im Auftrag eines Organisationskunden verarbeiten, bestimmt der Organisationskunde die Rechtsgrundlage der Verarbeitung. Unsere Verarbeitung erfolgt dann auf Grundlage des jeweiligen AVV und dokumentierter Weisungen.

5. Verarbeitete Daten und Zwecke

5.1 Kontodaten, Authentifizierung und Vertragsverwaltung

Bei Registrierung, Anmeldung und Nutzung eines EventCommand-Kontos verarbeiten wir insbesondere:

- Name und optional Vorname für die Anrede
- Login-E-Mail-Adresse und optionale abweichende Kommunikations-E-Mail-Adresse
- Telefonnummer, Firma/Organisation
- gehashtes Passwort über Supabase Auth; kein Klartextzugriff durch den Betreiber
- Zeitpunkte von Registrierung, letztem Login sowie E-Mail- oder Passwortänderungen
- Rollen- und Organisationszugehörigkeiten
- Zeitpunkte der Zustimmung zu AGB und, soweit einschlägig, AVV, einschließlich Organisation, akzeptierendem Nutzer, IP-Adresse und User-Agent als technische Nachweisdaten
- technische Authentifizierungs- und Sicherheitsereignisse

Zwecke sind die Bereitstellung des Nutzerkontos, Anmeldung, Zugriffsschutz, Organisationsverwaltung, Vertragsdurchführung, Missbrauchsprävention und Nachweis vertragsrelevanter Erklärungen. Rechtsgrundlagen sind Art. 6 Abs. 1 lit. b DSGVO, Art. 6 Abs. 1 lit. f DSGVO sowie Art. 6 Abs. 1 lit. c DSGVO, soweit gesetzliche Aufbewahrungs- oder Nachweispflichten bestehen.

IP-Adresse und User-Agent, die im Zusammenhang mit der Zustimmung bzw. Annahme von AGB und AVV gespeichert werden, verarbeiten wir ausschließlich zweckgebunden zum Nachweis dieser vertragsbezogenen Erklärung, zur Vertragsdokumentation sowie zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche. Eine Nutzung zu Tracking-, Marketing- oder Profiling-Zwecken findet nicht statt. Rechtsgrundlage ist Art. 6 Abs. 1 lit. b DSGVO, soweit die Verarbeitung für Abschluss und Durchführung des Vertrags erforderlich ist, sowie Art. 6 Abs. 1 lit. f DSGVO auf Grundlage unseres berechtigten Interesses an revisionssicherer Vertrags- und Nachweisdokumentation.

5.2 Organisations-, Event- und Betriebsdaten

Im Rahmen der Plattform können Organisationskunden insbesondere folgende Daten verwalten:

- Organisationsdaten wie Name, Slug, Tarif, Mitgliederliste, Rollen und Berechtigungen
- Eventdaten wie Name, Beschreibung, Datum, Status und Lebenszyklus
- Rollen, Organigramme, Zuständigkeiten und Besetzungen
- Kontaktdaten von Crew, Gästen, Freelancern und weiteren Zusatzkontakten, insbesondere Name, E-Mail-Adresse, Telefonnummer und Firma
- Schichtplanung, Ablaufplanung, Verfügbarkeiten und Zuordnungen
- Funkplanung und betriebliche Kommunikationsstrukturen
- Freigaben, Statusinformationen, Widerrufe und Begründungen
- Notfall- und Vorfalldokumentation einschließlich Protokollinformationen
- frei anlegbare Zusatzkontakte, teilweise mit eingeschränkter Sichtbarkeit
- von Gästen aktiv freigegebene Stammdaten als eventbezogener Snapshot
- Audit-Logs, insbesondere Nutzerkennung, Aktion, Zeitpunkt und betroffene Organisations- oder Eventstruktur
- hochgeladene PDF-Dokumente in privatem Supabase Storage

Diese Daten werden zur Bereitstellung der EventCommand-Funktionen verarbeitet, insbesondere Planung, Rollenverwaltung, Nachweisführung, Freigaben, Zugriffskontrolle, Dokumentation, Koordination und Sicherheitsorganisation. Soweit diese Daten durch Organisationskunden oder deren Nutzer für eigene Events verwaltet werden, verarbeitet EventCommand sie als Auftragsverarbeiter nach Art. 28 DSGVO.

5.3 Eingeladene Gäste, Freelancer und Stammdaten-Snapshot

Eingeladene Gäste, Freelancer oder Organisationsmitglieder können beim Beitritt zu einem Event bestimmte Stammdaten aktiv für das jeweilige Event freigeben. Dabei wird ein eventbezogener Snapshot der freigegebenen Daten erstellt, damit die Organisation die Daten für Rollenbesetzung, Kommunikation und Eventkoordination nutzen kann.

Die Freigabe betrifft nur die im Beitrittsprozess angezeigten Daten. Die Freigabe kann, soweit technisch vorgesehen und rechtlich möglich, für zukünftige Verwendungen widerrufen oder angepasst werden. Bereits für ein Event erforderliche Dokumentations- oder Nachweisdaten können durch den verantwortlichen Organisationskunden auf einer eigenen Rechtsgrundlage weiterverarbeitet werden.

5.4 Einladungssystem

Das Einladungssystem verarbeitet E-Mail-Adressen eingeladener Personen, Einladungscodes, Statusinformationen, einladende Person, Organisation/Event-Bezug und Zeitstempel. Die öffentliche Einladungsseite kann Organisationsnamen und Eventnamen anzeigen, damit eingeladene Personen die Einladung zuordnen können. Rechtsgrundlage für die Bereitstellung des Einladungssystems ist, soweit wir Verantwortlicher sind, Art. 6 Abs. 1 lit. b DSGVO; im Übrigen erfolgt die Verarbeitung im Auftrag des Organisationskunden.

5.5 Dokumente und Datei-Storage

Hochgeladene PDF-Dokumente werden in privatem Supabase Storage gespeichert. Der Abruf erfolgt nur für berechtigte Nutzer und grundsätzlich über signierte, zeitlich begrenzte URLs. Dokumente können personenbezogene Daten enthalten, soweit Organisationskunden oder berechtigte Nutzer solche Inhalte hochladen. In diesem Fall ist der jeweilige Organisationskunde für Rechtmäßigkeit, Datenminimierung, Zugriffsberechtigungen und Löschung verantwortlich.

5.6 Kalender-Abonnements (.ics)

Nutzer können Kalenderdaten über einen persönlichen .ics-Feed abonnieren. Der Zugriff erfolgt über einen nicht erratbaren Capability-Token. Der Feed enthält nur die für den jeweiligen Nutzer relevanten Schicht-, Ablauf- oder Zeitplandaten und keine fremden Kontaktdaten.

Der Token ist wie ein vertraulicher Link zu behandeln. Wer Zugriff auf den Link erhält, kann die darin enthaltenen Kalenderdaten abrufen. Nutzer können den Token, soweit technisch vorgesehen, deaktivieren oder neu erzeugen. Beim Einbinden des Feeds in externe Kalenderanwendungen können diese Anbieter eigene personenbezogene Daten verarbeiten; hierfür gelten die Datenschutzbedingungen des jeweiligen Kalenderanbieters. Rechtsgrundlage ist Art. 6 Abs. 1 lit. b DSGVO sowie Art. 6 Abs. 1 lit. f DSGVO für Missbrauchsprävention und technische Absicherung.

5.7 E-Mail-Versand: Service-Mails und Marketing-Mails

Wir versenden E-Mails, die für Betrieb und Nutzung von EventCommand erforderlich sind. Dazu gehören insbesondere Einladungen, Authentifizierungs- und Bestätigungs-E-Mails, Passwortzurücksetzungen, E-Mail-Änderungen, sicherheitsrelevante Hinweise sowie vertrags- oder funktionsbezogene Benachrichtigungen.

Für diese Service-Mails verarbeiten wir insbesondere Empfängeradresse, Name, Organisation/Event-Bezug, Versandzeitpunkt, Zustellstatus sowie erforderliche Sicherheits- oder Bestätigungslinks. Rechtsgrundlagen sind Art. 6 Abs. 1 lit. b DSGVO für vertrags- und funktionsnotwendige E-Mails sowie Art. 6 Abs. 1 lit. f DSGVO für Sicherheits- und Zustellnachweise.

Optional versenden wir Produktinformationen, Release-Hinweise und Marketing-/Produkt-News nur, wenn hierfür eine aktive Einwilligung vorliegt oder eine gesetzliche Ausnahme im Einzelfall greift. Die Marketing-Checkbox ist nicht vorausgewählt. Wir speichern Einwilligungsstatus, Zeitpunkt, Quelle und Inhalt der Einwilligung sowie einen Abmelde-Token. Jede Marketing-E-Mail enthält einen Abmeldelink. Der Widerruf ist jederzeit mit Wirkung für die Zukunft möglich und berührt nicht die Zulässigkeit bereits erfolgter Verarbeitung. Service-Mails, die für Konto, Sicherheit oder Vertragsdurchführung erforderlich sind, werden unabhängig von einer Marketing-Abmeldung versendet.

Rechtsgrundlage für Marketing-Mails ist Art. 6 Abs. 1 lit. a DSGVO. Zusätzlich beachten wir die Anforderungen des § 7 UWG für Werbung per elektronischer Post. EventCommand nutzt keine Öffnungs- oder Klicktracking-Funktionen in E-Mails. Falls solche Funktionen künftig eingesetzt werden, wird diese Datenschutzerklärung vorab aktualisiert.

5.8 Newsletter und Bezug kostenloser Materialien (Lead-Funnel)

Über Formulare auf unserer Website (Startseite, Wissensartikel) können Sie kostenlose Materialien (z.B. das „Organigramm-Vorlagenpaket“) anfordern und optional unseren Praxis-Tipp-Newsletter abonnieren.

Verarbeitete Daten: E-Mail-Adresse (Pflicht) sowie freiwillig Vorname, Firma und Funktion. Zusätzlich protokollieren wir zum Nachweis der Einwilligung jeweils Datum und Uhrzeit, IP-Adresse und Browserkennung (User-Agent) sowohl bei der Anmeldung als auch bei der Bestätigung.

Zweck und Rechtsgrundlage: Zusendung des angeforderten Materials und, bei separater Einwilligung, regelmäßiger fachlicher Hinweise per E-Mail. Rechtsgrundlage ist Ihre Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO. Wir verwenden das Double-Opt-in-Verfahren: Nach der Anmeldung erhalten Sie eine E-Mail mit einem Bestätigungslink; erst nach Ihrer Bestätigung senden wir das Material bzw. nehmen Sie in den Newsletter auf.

Auftragsverarbeiter: Der E-Mail-Versand erfolgt über Resend (Plus Five Five, Inc., USA) mit EU-Versandregion Irland (AWS eu-west-1). Mit dem Anbieter besteht ein Auftragsverarbeitungsvertrag nach Art. 28 DSGVO. Da Resend ein US-Unternehmen ist, können Account-, Log- und E-Mail-Metadaten in den USA verarbeitet werden; die Übermittlung erfolgt auf Basis der EU-Standardvertragsklauseln (SCC) sowie, soweit einschlägig, des EU-US Data Privacy Framework. Näheres regelt Abschnitt 6.

Speicherdauer: Nicht bestätigte Anmeldungen werden spätestens nach 30 Tagen automatisch gelöscht. Bestätigte Datensätze speichern wir bis zum Widerruf Ihrer Einwilligung. Wird Ihre Anmeldung in ein Nutzerkonto überführt, bleibt der Datensatz mit dem Konto verknüpft.

Widerruf: Sie können Ihre Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen, insbesondere über den Abmeldelink am Ende jeder E-Mail. Nach dem Widerruf bewahren wir zur Sicherstellung, dass Sie keine weiteren E-Mails erhalten, lediglich einen kryptografischen Hash Ihrer E-Mail-Adresse sowie das Datum des Widerrufs in einer Sperrliste auf (berechtigtes Interesse, Art. 6 Abs. 1 lit. f DSGVO); alle übrigen zu Ihnen gespeicherten Daten werden gelöscht.

5.9 Push-Benachrichtigungen

EventCommand versendet Push-Benachrichtigungen an Geräte von Nutzern, die diese aktiv aktiviert haben. Push-Benachrichtigungen werden über Web-Push in der installierbaren Web-App (PWA) sowie über die nativen Apps (Android in Vorbereitung, iOS geplant) ausgeliefert. Ausgelöst werden sie bei Notfällen, Freigaben, Schicht-Anfragen, Einladungen und Sicherheitsunterweisungen.

Verwendete Push-Dienste: Für die technische Zustellung nutzen wir die Push-Infrastruktur der Betriebssystem- und Browserhersteller:

- Google (Firebase Cloud Messaging) – Google Ireland Ltd., Irland, sowie Google LLC, USA. Genutzt für Push an Chrome und die Android-App.
- Apple (Apple Push Notification service) – Apple Distribution International Ltd., Irland, sowie Apple Inc., USA. Genutzt für Push an Safari (iOS/macOS) und die iOS-App.
- Mozilla – für Web-Push an den Firefox-Browser.

Verarbeitete Daten: ein gerätebezogener Push-Token (FCM-Registration-Token bzw. APNs-Device-Token – eine Gerätekennung) sowie der Benachrichtigungsinhalt (kurze Überschrift, kurzer Text und ein In-App-Link zum betroffenen Bereich). Der Inhalt wird bewusst knapp und ohne sensible oder unnötige personenbezogene Details gehalten. Besondere Kategorien personenbezogener Daten werden über Push nicht übermittelt.

Zweck: technische Zustellung der vom Nutzer aktivierten Benachrichtigungen an sein Gerät.

Rechtsgrundlage: Ihre Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO, die Sie über den Berechtigungsdialog des Betriebssystems bzw. Browsers und die App-Einstellungen (Einstellungen → Benachrichtigungen, Kanal je Kategorie) erteilen. Hilfsweise stützen wir die Verarbeitung auf Art. 6 Abs. 1 lit. b und lit. f DSGVO, soweit die Benachrichtigung der Vertragsdurchführung oder der Koordination im Rahmen der Veranstaltungsorganisation dient.

Drittlandübermittlung USA: Bei der Zustellung können Push-Token und Benachrichtigungsinhalte an die genannten US-Anbieter übermittelt werden. Google und Apple sind unter dem EU-US Data Privacy Framework zertifiziert; ergänzend gelten die EU-Standardvertragsklauseln. Näheres regelt Abschnitt 6. Push-Benachrichtigungen sind der einzige bewusste Verarbeitungspunkt außerhalb der EU; die übrige Datenverarbeitung erfolgt in EU-Regionen.

Speicherdauer: Der Push-Token wird gespeichert, bis Sie Benachrichtigungen deaktivieren, sich abmelden, die App deinstallieren oder der Token ungültig wird; danach wird er automatisch gelöscht.

Widerruf: Sie können Ihre Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen – über die Benachrichtigungseinstellungen Ihres Betriebssystems bzw. Browsers sowie in der App unter Einstellungen → Benachrichtigungen.

5.10 Rechnungs- und Vertragsdaten

Da keine Zahlungsabwicklung in der App stattfindet, werden Zahlungsdaten nicht über EventCommand verarbeitet. Für manuelle Rechnungstellung und Vertragsverwaltung verarbeiten wir insbesondere Name und Firma des Rechnungsempfängers, Rechnungsadresse, Tarif, Laufzeit, Abrechnungszeitraum, gegebenenfalls Umsatzsteuer-Identifikationsnummer sowie vertragsbezogene Kommunikation. Rechtsgrundlagen sind Art. 6 Abs. 1 lit. b DSGVO und Art. 6 Abs. 1 lit. c DSGVO.

5.11 Server-Logs, technische Zugriffsdaten und Sicherheit

Beim Zugriff auf EventCommand werden technische Daten verarbeitet, insbesondere IP-Adresse, Datum und Uhrzeit des Zugriffs, aufgerufene URL, Browser-Typ, Betriebssystem, HTTP-Statuscode, Request-Metadaten und sicherheitsrelevante Ereignisse. Zwecke sind Sicherstellung des Betriebs, Fehleranalyse, Abwehr von Angriffen, Zugriffsschutz und Missbrauchsprävention. Rechtsgrundlage ist Art. 6 Abs. 1 lit. f DSGVO.

5.12 Admin-Zugriff und Support

Der Betreiber verfügt über administrative Zugriffsmöglichkeiten für Support, Sicherheitsprüfung, Tarifverwaltung, Fehleranalyse, Mitgliederverwaltung sowie Löschung von Accounts oder Organisationen. Der Zugriff ist auf den Betreiber beschränkt, wird nur bei Supportanfragen, Sicherheitsvorfällen, betrieblichen Notwendigkeiten oder rechtlich erforderlichen Maßnahmen genutzt und protokolliert. Rechtsgrundlage ist Art. 6 Abs. 1 lit. f DSGVO; bei Kundendaten erfolgt der Zugriff im Rahmen des AVV und nach dokumentierter Weisung oder zur Vertragserfüllung erforderlicher Nebenpflichten.

5.13 Notfall- und Vorfalldokumentation; besondere Kategorien personenbezogener Daten

EventCommand stellt Funktionen zur sachbezogenen Dokumentation von Notfällen, Störungen und Vorfällen bei Veranstaltungen bereit. Die Funktion ist auf organisatorische Informationen wie Zeitpunkt, Ort, Maßnahmen, Zuständigkeiten, Status und Verlauf ausgelegt.

Die Eingabe besonderer Kategorien personenbezogener Daten, insbesondere Gesundheitsdaten, Diagnosen, Verletzungsdetails oder medizinische Behandlungen einzelner Personen, ist von EventCommand nicht vorgesehen. Organisationskunden sind verpflichtet, vor der Eingabe solcher Daten eigenständig zu prüfen, ob hierfür eine tragfähige Rechtsgrundlage nach Art. 6 DSGVO und eine Ausnahme nach Art. 9 DSGVO besteht.

Soweit Organisationskunden dennoch personenbezogene oder besondere Kategorien personenbezogener Daten in Vorfallprotokollen verarbeiten, erfolgt die Verarbeitung durch EventCommand ausschließlich im Auftrag und nach Weisung des jeweiligen Organisationskunden. Der Organisationskunde bleibt für Rechtmäßigkeit, Informationspflichten, Datenminimierung, Zugriffsbeschränkung und Löschung verantwortlich.

6. Hosting, Auftragsverarbeiter und Drittlandübermittlungen

Zur Bereitstellung von EventCommand setzen wir spezialisierte Dienstleister ein, die personenbezogene Daten in unserem Auftrag oder als Unterauftragsverarbeiter verarbeiten. Mit Vercel, Supabase und Resend bestehen Vereinbarungen zur Auftragsverarbeitung bzw. Data Processing Addenda. Für die Zustellung von Push-Benachrichtigungen (siehe Abschnitt 5.9) kommen zusätzlich Google und Apple zum Einsatz. Die technische Produktkonfiguration ist auf EU-Regionen für produktive App-Funktionen ausgerichtet; gleichwohl können aufgrund der eingesetzten US-Anbieter, deren Account-/Service-Daten, Support-, Sicherheits- und Subprozessorstrukturen sowie E-Mail-Metadaten Drittlandübermittlungen in die USA oder Zugriffe aus Drittländern nicht ausgeschlossen werden.

Dienstleister	Zweck	Region/Verarbeitung	Transfermechanismus
Vercel Inc., USA	Hosting des Frontends, CDN, Build-Pipeline, Serverless-Funktionen	Serverless-Funktionen sind für EventCommand auf fra1 Frankfurt/EU konfiguriert; statische Inhalte können über ein globales CDN ausgeliefert werden.	DPA; EU-US Data Privacy Framework und, soweit erforderlich, Standardvertragsklauseln bzw. weitere Transfermechanismen des Vercel-DPA.
Supabase Inc., USA	PostgreSQL-Datenbank, Authentifizierung, privater Datei-Storage, Zugriffskontrolle	Projektregion eu-central-1 Frankfurt/EU.	DPA; Standardvertragsklauseln bzw. Transfermechanismen des Supabase-DPA.
Resend / Plus Five Five, Inc., USA	Versand von Service-Mails und optionalen Marketing-/Produkt-News	Versandregion eu-west-1 Irland. Nach Anbieterinformation steuert diese Region den Versandweg; Accountdaten, E-Mail-Metadaten, Logs und API-Records können in den USA gespeichert werden.	DPA; EU-US Data Privacy Framework und Standardvertragsklauseln nach Resend-DPA.
Google Ireland Ltd., Irland / Google LLC, USA	Push-Zustellung (Firebase Cloud Messaging) an Chrome und die Android-App	Zustellung über Google-Infrastruktur; Verarbeitung auch in den USA möglich.	EU-US Data Privacy Framework; ergänzend Standardvertragsklauseln.
Apple Distribution International Ltd., Irland / Apple Inc., USA	Push-Zustellung (Apple Push Notification service) an Safari (iOS/macOS) und die iOS-App	Zustellung über Apple-Infrastruktur; Verarbeitung auch in den USA möglich.	EU-US Data Privacy Framework; ergänzend Standardvertragsklauseln.

Eine darüber hinausgehende Weitergabe personenbezogener Daten erfolgt nur, wenn dies zur Vertragserfüllung erforderlich ist, wir gesetzlich verpflichtet sind oder eine Einwilligung vorliegt. Ein Verkauf personenbezogener Daten findet nicht statt.

7. Speicherdauer und Löschkonzept

Datenkategorie	Speicherdauer/Kriterien
Account- und Profildaten	Bis zur Löschung des Nutzerkontos; danach Löschung oder Anonymisierung, soweit keine gesetzlichen Aufbewahrungspflichten oder berechtigten Nachweisinteressen entgegenstehen. Daten, die Bestandteil von Organisations- oder Eventinhalten sind, werden nach Weisung des Organisationskunden behandelt.
AGB-/AVV-Zustimmungen	Für die Dauer des Vertragsverhältnisses und anschließend für gesetzliche Verjährungs- und Nachweisfristen. Die zugehörigen Nachweisdaten (Zeitpunkt, Organisation, akzeptierender Nutzer, IP-Adresse und User-Agent) werden ausschließlich zum Nachweis der AGB-/AVV-Annahme, zur Vertragsdokumentation und zur Verteidigung oder Durchsetzung rechtlicher Ansprüche gespeichert. Regelmäßig erfolgt die Speicherung bis zum Ablauf von drei Jahren nach Ende des Jahres, in dem das Vertragsverhältnis endet; bei laufenden Ansprüchen, Streitigkeiten oder gesetzlichen Aufbewahrungspflichten entsprechend länger.
Organisations- und Eventdaten	Bis zur Löschung durch den Org-Owner oder bis zur Löschung nach Vertragsende. Nach Vertragsende kann eine Übergangsfrist von bis zu 30 Tagen für Export und Wiederherstellung bestehen.
Kontaktdaten (Crew, Gäste, Freelancer, Zusatzkontakte)	Bis zur Löschung durch den Organisationskunden oder bis zur Löschung der zugehörigen Organisation bzw. des Events.
Gäste-Snapshots	Bis zur Löschung durch den Organisationskunden, bis zur Entfernung aus dem Event oder bis zur Löschung des zugehörigen Events, soweit keine längeren Aufbewahrungsgründe bestehen.
Hochgeladene Dokumente	Bis zur Löschung durch berechtigte Nutzer oder bis zur Löschung der Organisation bzw. des Events.
Einladungen und Einladungstokens	Bis zur Annahme, Ablehnung, zum Ablauf oder zur Rücknahme der Einladung; spätestens mit Löschung der Organisation bzw. des Events.
Kalender-Feeds und Capability-Tokens	Bis zur Deaktivierung, Neuerzeugung oder Löschung des Nutzerkontos bzw. der zugehörigen Organisation.
Audit-Logs	Für die Dauer, die für Sicherheit, Nachvollziehbarkeit und Missbrauchsprävention erforderlich ist. Zielwert: regelmäßig 12 Monate, sofern keine längeren Nachweisinteressen bestehen.
Marketing-Einwilligungen	Bis zum Widerruf. Nach Widerruf speichern wir die Abmeldeinformation, soweit dies erforderlich ist, um künftige Marketing-Mails zu verhindern und die Abmeldung nachzuweisen.
E-Mail-Zustelldaten	Für betriebliche Zustell- und Fehleranalyse nur solange erforderlich. Resend kann Daten nach den Bedingungen des Resend-DPA und der Produktkonfiguration speichern.
Server- und Sicherheitslogs	Regelmäßig bis zu 30 Tage, sofern keine längere Speicherung zur Aufklärung von Sicherheitsvorfällen erforderlich ist.
Backups	Zur Wiederherstellung nach Datenverlust erstellen wir regelmäßig Sicherungskopien der Anwendungsdaten (Nutzerkonten, Events, Rollen, Kontakte, hochgeladene Dokumente). Diese werden verschlüsselt gespeichert und nach 30 Tagen automatisch gelöscht. Soweit der eingesetzte Datenbank-Anbieter eigene Backups bereitstellt, richtet sich deren Aufbewahrung nach den Routinen des Anbieters.

Rechnungs- und Buchhaltungsdaten	10 Jahre gemäß steuer- und handelsrechtlichen Aufbewahrungspflichten.

Datensicherung und Löschung: Löscht eine Organisation ihre Daten oder verlangen Sie die Löschung, werden die Daten unverzüglich aus der Live-Datenbank gelöscht. In Datensicherungen verbleiben sie technisch bedingt noch bis zu 30 Tage und werden danach automatisch gelöscht. In dieser Zeit werden die Sicherungen ausschließlich zur Wiederherstellung nach Datenverlust verwendet, nicht für andere Zwecke genutzt und nur vom Betreiber eingesehen. Muss eine Sicherung zurückgespielt werden, werden bereits gelöschte Daten unverzüglich erneut gelöscht.

8. Rechte betroffener Personen

Betroffene Personen haben nach Maßgabe der DSGVO Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit, Widerspruch sowie Widerruf erteilter Einwilligungen.

Soweit wir personenbezogene Daten als Verantwortlicher verarbeiten, bearbeiten wir entsprechende Anfragen direkt. Soweit wir personenbezogene Daten im Auftrag eines Organisationskunden verarbeiten, ist grundsätzlich der jeweilige Organisationskunde für die Beantwortung der Anfrage verantwortlich. In solchen Fällen leiten wir die Anfrage an den Organisationskunden weiter oder unterstützen ihn nach Maßgabe des AVV.

Einwilligungen in Marketing-Mails können jederzeit über den Abmeldelink in jeder Marketing-E-Mail oder per Nachricht an uns widerrufen werden. Der Widerruf wirkt für die Zukunft. Bei Verarbeitungen auf Grundlage berechtigter Interessen besteht ein Widerspruchsrecht nach Art. 21 DSGVO. Bei Direktwerbung werden personenbezogene Daten nach Widerspruch nicht mehr für diesen Zweck verarbeitet.

Zur Ausübung Ihrer Rechte oder für einen Datenexport: support [at] eventcommand [punkt] de

9. Beschwerderecht bei der Aufsichtsbehörde

Betroffene Personen haben das Recht, sich bei einer Datenschutzaufsichtsbehörde zu beschweren. Für den Betreiber ist nach aktuellem Stand zuständig:

Berliner Beauftragte für Datenschutz und Informationsfreiheit

Alt-Moabit 59-61, 10555 Berlin

E-Mail: mailbox@datenschutz-berlin.de | Website: https://www.datenschutz-berlin.de

10. Datensicherheit

Wir und unsere Auftragsverarbeiter setzen technische und organisatorische Maßnahmen ein, um personenbezogene Daten gegen Verlust, Missbrauch, unbefugten Zugriff und unbefugte Offenlegung zu schützen. Dazu gehören insbesondere:

- verschlüsselte Übertragung per TLS/HTTPS
- Passworthashing über Supabase Auth; keine Speicherung von Klartextpasswörtern
- Row Level Security (RLS) und rollenbasierte Zugriffskontrolle
- private Dateiablage und signierte, zeitlich begrenzte Download-URLs
- mandantenbezogene Trennung von Organisationsdaten

- administrativer Zugriff nur für betriebliche, sicherheitsbezogene oder supportbezogene Zwecke
- Protokollierung sicherheits- und nachweisrelevanter Aktionen
- regelmäßige, verschlüsselt gespeicherte Datensicherungen mit begrenzter Aufbewahrungsdauer (siehe Abschnitt 7) sowie plan- und anbieterabhängige Backups und Wiederherstellungsmechanismen

11. Cookies und lokale Speicherung

EventCommand verwendet ausschließlich technisch notwendige Cookies und vergleichbare lokale Speicherungen, die für Anmeldung, Sitzungsverwaltung, Zugriffsschutz und Bereitstellung der ausdrücklich gewünschten App-Funktionen erforderlich sind. Hierzu gehören insbesondere Authentifizierungs- und Session-Informationen von Supabase Auth.

Rechtsgrundlage für die Speicherung bzw. den Zugriff auf Informationen in der Endeinrichtung ist § 25 Abs. 2 Nr. 2 TDDDG. Eine Einwilligung und ein Consent-Banner sind hierfür nicht erforderlich.

Analyse-Cookies, Marketing-Cookies, Werbenetzwerke, Drittanbieter-Tracking sowie Öffnungs- oder Klicktracking in E-Mails werden nicht eingesetzt. Werden technisch notwendige Speicherungen im Browser deaktiviert, kann die App nicht oder nur eingeschränkt genutzt werden.

12. Testphase und Tarifwechsel

Neue Organisationen können einmalig eine 14-tägige Testphase im COMMAND-Tarif nutzen. Nach Ablauf wird die Organisation in einen eingeschränkten Zustand versetzt: bestehende Daten sind weiterhin lesbar, neue Daten können erst nach Auswahl eines gültigen Tarifs eingepflegt werden. Tarifwechsel und Upgrades erfolgen außerhalb der App persönlich oder per E-Mail.

13. Automatisierte Entscheidungen und Profiling

EventCommand setzt keine automatisierten Entscheidungen im Sinne von Art. 22 DSGVO und kein Profiling ein.

14. Änderungen dieser Datenschutzerklärung

Wir behalten uns vor, diese Datenschutzerklärung zu aktualisieren, wenn sich Funktionen, technische Dienstleister, Rechtslage oder Verarbeitungsabläufe ändern. Die jeweils aktuelle Version ist unter https://eventcommand.de einsehbar. Bei wesentlichen Änderungen werden registrierte Nutzer per E-Mail informiert.

Version 1.5 · Stand: 26. Oktober 2026