

# Vercel Data Processing Agreement (DPA)

Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO — Stand: Last Updated 31.03.2023 — Quelle: <https://vercel.com/legal/dpa>

## Hinweis zur Geltung

Vercel stellt das Data Processing Addendum als öffentliches Vertragsdokument bereit. Es wird mit Vertragsabschluss bzw. Nutzungsbeginn der Dienste automatisch Bestandteil der Vertragsbeziehung. Eine separate Unterschrift ist im Standardfall nicht erforderlich. Dieses PDF dient als Nachweis und Archivkopie für die EA-Compliance-Ablage. Wenn ein vom Anbieter unterzeichnetes DPA benötigt wird (z. B. auf Kundenanforderung), kann dieses über [privacy@vercel.com](mailto:privacy@vercel.com) angefordert werden.

## 1. Einleitung

Dieses Data Processing Addendum ("Addendum") ergänzt den Vercel Enterprise Services Order Form, die Enterprise Terms and Conditions oder eine andere zwischen Vercel und dem Kunden geschlossene Vereinbarung über die Bereitstellung der Dienste (die "Vereinbarung") und ist Bestandteil dieser. Vertragspartner sind Vercel Inc., eine Gesellschaft mit Sitz in Delaware, und der Kunde, der die Vereinbarung abgeschlossen hat. Das Addendum gilt für die Verarbeitung personenbezogener Daten durch Vercel im Rahmen der Vereinbarung. Das Addendum wird mit Abschluss der Vereinbarung rechtlich verbindlich.

## 2. Definitionen (Auszug)

**Anwendbare Datenschutzgesetze.** Alle einschlägigen Datenschutzgesetze und -verordnungen, einschließlich EU-DSGVO 2016/679, UK Data Protection Act 2018, CCPA (Kalifornien), PIPEDA (Kanada) sowie der Australian Privacy Act (1988).

**Customer Data.** Personenbezogene Daten, die Vercel im Auftrag des Kunden verarbeitet.

**Service-Generated Data.** Nutzungs- und Metadaten, die durch die Inanspruchnahme der Dienste entstehen. Soweit es sich um personenbezogene Daten handelt, verarbeitet Vercel diese als Verantwortlicher.

**Subprocessor.** Jeder von Vercel beauftragte Dritte, der Customer Data zur Erbringung der Dienste verarbeitet.

**Security Incident.** Jede bestätigte unbefugte oder rechtswidrige Verletzung der Sicherheit, die zu unbeabsichtigter oder rechtswidriger Vernichtung, Verlust, Veränderung oder unbefugter Offenlegung führt.

## 3. Rolle der Parteien

**Vercel als Auftragsverarbeiter.** Hinsichtlich der Verarbeitung von Customer Data handelt der Kunde als Verantwortlicher (oder ggf. selbst als Auftragsverarbeiter), Vercel als Auftragsverarbeiter. Vercel verarbeitet Customer Data ausschließlich nach den dokumentierten, rechtmäßigen Weisungen des Kunden im Rahmen der Vereinbarung.

**Vercel als Verantwortlicher.** In Bezug auf Service-Generated Data und Contact Data handelt Vercel als Verantwortlicher und verarbeitet diese Daten gemäß der Vercel Privacy Policy.

## 4. Subprocessing

Der Kunde ermächtigt Vercel ausdrücklich, verbundene Unternehmen (Affiliates) und allgemein Subprocessor mit der Verarbeitung von Customer Data zu beauftragen. Vercel schließt mit jedem Subprocessor eine schriftliche Vereinbarung mit Datenschutzpflichten, die im Wesentlichen denen dieses Addendums entsprechen, und haftet für Pflichtverletzungen seiner Subprocessor. Eine aktuelle Liste der Subprocessor ist unter [security.vercel.com](https://security.vercel.com) einsehbar. Über neue Subprocessor wird auf Anforderung an [privacy@vercel.com](mailto:privacy@vercel.com) per E-Mail informiert. Widerspruchsfrist: 5 Kalendertage.

## 5. Sicherheit

Vercel implementiert und unterhält technische und organisatorische Maßnahmen (TOMs) zum Schutz der Customer Data. Hierzu gehören u. a. Verschlüsselung im Ruhezustand (AES-256) und in der Übertragung (TLS 1.2 oder höher), strenge Zugriffskontrollen nach dem Least-Privilege-Prinzip, regelmäßige Backups in mehreren Verfügbarkeitszonen, jährliche Sicherheitstrainings für Mitarbeitende sowie unabhängige Audits (SOC 2 Type 2, jährlich). Bei einem bestätigten Security Incident benachrichtigt Vercel den Kunden ohne unangemessene Verzögerung.

## 6. Audit-Rechte

Vercel beauftragt mindestens einmal jährlich externe Auditoren, die die Angemessenheit der Sicherheitsmaßnahmen prüfen (z. B. SOC 2 Type 2). Auf schriftliche Anfrage des Kunden in zumutbaren Abständen und unter Wahrung angemessener Vertraulichkeitspflichten stellt Vercel eine Kopie des aktuellsten Audit-Berichts zur Verfügung. Der Kunde stimmt zu, dass durch diese Berichte sämtliche Audit-Rechte aus den anwendbaren Datenschutzgesetzen erfüllt werden.

## 7. Betroffenenrechte

Vercel unterstützt den Kunden auf Anfrage und auf dessen Kosten in angemessenem Umfang bei der Erfüllung seiner Pflichten zur Beantwortung von Betroffenenanfragen (Auskunft, Berichtigung, Löschung, Einschränkung, Übertragbarkeit, Widerspruch). Wendet sich eine betroffene Person direkt an Vercel, verweist Vercel diese an den Kunden; der Kunde ist für die Beantwortung verantwortlich.

## 8. Rückgabe oder Löschung

Der Kunde kann Customer Data jederzeit über die Self-Service-Funktionen der Dienste löschen oder exportieren. Die Beendigung der Vereinbarung gilt als Anweisung zur Löschung aller Customer Data innerhalb einer wirtschaftlich vertretbaren Frist, soweit keine gesetzliche Aufbewahrungspflicht entgegensteht.

## 9. Internationale Datenübermittlung

Die primären Verarbeitungsstätten von Vercel befinden sich in den Vereinigten Staaten. Vercel kann Customer Data in die USA und in andere Länder übermitteln, in denen Vercel oder seine Subprocessor Verarbeitungsstätten unterhalten. Solche Übermittlungen erfolgen in Übereinstimmung mit den anwendbaren Datenschutzgesetzen und diesem Addendum.

Für Übermittlungen aus dem EWR, dem Vereinigten Königreich und der Schweiz kommen die EU-Standardvertragsklauseln 2021 (Beschluss (EU) 2021/914) sowie das UK International Data Transfer Addendum (IDTA) zur Anwendung. Die anwendbaren Module (Module 1, 2 oder 3) richten sich nach der Rolle der Parteien im jeweiligen Datenstrom. Die zuständige Aufsichtsbehörde im Sinne der SCCs ist die irische Data Protection Commission. Streitigkeiten unterliegen irischem Recht und der Gerichtsbarkeit Irlands.

Vercel ist zusätzlich unter dem EU-US Data Privacy Framework, der UK-Erweiterung sowie dem Swiss-US DPF beim US-Handelsministerium zertifiziert.

## Schedule 1 — Subject Matter & Details of Processing

<b>Gegenstand</b>	Bereitstellung der Vercel-Dienste (Frontend Cloud)
<b>Art und Zweck</b>	Verarbeitung personenbezogener Daten zur Erbringung der Dienste, Hosting, Auslieferung von Inhalten
<b>Dauer</b>	Für die Laufzeit der Vereinbarung; Customer Data wird nach Beendigung gelöscht (siehe Ziff. 8).
<b>Betroffene Personen</b>	Endnutzer des Kunden, autorisierte Nutzer mit Vercel-Zugang, Lieferanten und Mitarbeitende des Kunden
<b>Datenkategorien</b>	Vom Kunden bestimmt; typisch: IP-Adressen, Systemkonfigurationsinformationen, ggf. weitere Daten
<b>Sensitive Daten</b>	Die Verarbeitung sensibler Daten oder besonderer Kategorien personenbezogener Daten ist dem Kunden vorbehalten

## Schedule 2 — Technical & Organizational Measures (Kurzfassung)

**Pseudonymisierung & Verschlüsselung.** AES-256 im Ruhezustand, TLS 1.2+ in der Übertragung. AWS KMS für Schlüsselmanagement (FIPS 140-2 validiert).

**Vertraulichkeit & Verfügbarkeit.** Strenge Vertraulichkeitsverpflichtungen für Mitarbeitende und Subprocessor. Mehrere fault-independent Availability Zones bei AWS, Azure und GCP. Regelmäßige Backups, repliziert über Regionen.

**Wiederherstellung.** Business Continuity- und Disaster-Recovery-Plan. Backups verschlüsselt, redundant über Verfügbarkeitszonen verteilt, periodisch getestet.

**Tests & Audits.** Risikobasiertes Sicherheitsprogramm. Jährliche unabhängige Audits (SOC 2 Type 2), Penetrationstests, Vulnerability Scanning.

**Identifikation & Berechtigung.** Eindeutige Anmeldedaten, Least-Privilege-Prinzip, rollen- und zeitbasierte Zugriffsmodelle, Entzug bei Rollenwechsel/Austritt.

**Übertragung & Speicherung.** Verschlüsselung in Transit und Storage (AES-256). AWS KMS für Schlüssel.

**Physische Sicherheit.** Vercel ist Remote-First; Hosting auf AWS, Azure, GCP mit deren physischen Sicherheitskontrollen.

**Logging.** Zentrales Sicherheits-Monitoring durch das Security-Team; Aktivitätsprotokolle für Kunden über Activity Log verfügbar.

**Konfiguration.** Secure SDLC, jährliche Pentests, Change-Management-Prozess für Produktivumgebungen.

**IT-Governance.** Dediziertes Information-Security-Team; Policies werden jährlich von der Geschäftsleitung überprüft.

**Zertifizierungen.** SOC 2 Type 2, ISO/IEC 27001, PCI DSS, HIPAA, GDPR, EU-US/Swiss-US/UK Data Privacy Framework, TISAX AL2, NIS 2, DORA u. a.

**Datenminimierung & -qualität.** Shared-Responsibility-Modell; Kunden bestimmen Inhalte. Self-Service-Funktionen für Löschung. Unit-, Volume- und End-to-End-Tests.

**Aufbewahrung.** Nach Vertragsende Löschung innerhalb wirtschaftlich vertretbarer Frist, soweit keine gesetzliche Aufbewahrungspflicht entgegensteht.

**Subprocessor-Maßnahmen.** Schriftliche Verträge mit substantiell gleichwertigen Pflichten. Meldepflicht bei Security Incidents, Löschung auf Anweisung, keine weiteren Subprocessor ohne Genehmigung.

## Schedule 3 — Internationale Datenübermittlung

Für Datenübermittlungen aus dem EWR, dem Vereinigten Königreich und der Schweiz kommen die 2021 EU Standard Contractual Clauses zur Anwendung. Anwendbare Module:

**Modul 1 (Controller-Controller):** Wenn Kunde und Vercel jeweils Verantwortliche sind (z. B. für Service-Generated Data oder Contact Data).

**Modul 2 (Controller-Processor):** Wenn der Kunde Verantwortlicher und Vercel Auftragsverarbeiter ist (Standardfall für Customer Data).

**Modul 3 (Processor-Processor):** Wenn der Kunde selbst Auftragsverarbeiter und Vercel Sub-Auftragsverarbeiter ist.

Klauseln im Detail: Klausel 7 (Andocken) gilt nicht. In Klausel 9 gilt Option 2 mit der Vorlaufzeit gemäß Ziffer 7 (Subprocessing). Optionale Sprache in Klausel 11 entfällt. Anwendbares Recht (Klausel 17): irisches Recht. Gerichtsstand (Klausel 18b): Irland. Zuständige Aufsichtsbehörde: Irish Data Protection Commission.

## Schedule 4 — Jurisdiktionsspezifische Bestimmungen

Spezifische Anpassungen für Kalifornien (CCPA), EWR (DSGVO), Schweiz (FADP), Vereinigtes Königreich (UK GDPR + DPA 2018), Australien (Privacy Act 1988) und Kanada (PIPEDA). Im EWR: Bei Beauftragung von Subprocessor verpflichtet Vercel diese auf einen Schutzstandard gemäß Art. 28 Abs. 3 DSGVO. GDPR-Bußgelder gemäß Art. 83 sind nicht über die Haftungsregelungen der Vereinbarung indemnifiziert.

## Schedule 5 — UK IDTA (Kurzfassung)

Für Datenübermittlungen aus dem Vereinigten Königreich gilt das UK International Data Transfer Addendum (IDTA) der ICO in Verbindung mit den EU-SCCs. Importeur: Vercel Inc., 440 N Barranca Ave #4133, Covina, CA 91723, Delaware-Registernummer 5857312. Kontakt: [privacy@vercel.com](mailto:privacy@vercel.com). Anwendbares Recht: England und Wales.

Diese Zusammenfassung wurde am 29.04.2026 für die Compliance-Ablage von Essential Advertising erstellt. Der vollständige Originaltext ist die maßgebliche Fassung und unter <https://vercel.com/legal/dpa> abrufbar. Für jede Vertragsbeziehung ist die zum jeweiligen Stichtag gültige Vercel-Fassung einschlägig.