

Muster-Auftragsverarbeitungsvertrag (Art. 28 DSGVO)

Stand: 26. November 2025 · Muster — im Einzelfall an das konkrete Projekt anzupassen.

zwischen

Auftraggeber (Verantwortlicher i. S. v. Art. 4 Nr. 7 DSGVO):

Firma, Anschrift, gesetzlicher Vertreter: _____

– nachfolgend „Verantwortlicher“ –

und

Auftragsverarbeiter (i. S. v. Art. 4 Nr. 8 DSGVO):

Stadtbewohner Webdesign | Björn Becker

Aarstraße 222, 65232 Taunusstein-Wehen, Deutschland

– nachfolgend „Auftragsverarbeiter“ –

§ 1 Gegenstand und Dauer

(1) Gegenstand dieses Vertrages ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen im Rahmen der zwischen den Parteien vereinbarten Leistungen (Hauptvertrag: Web-, Software- oder KI-Projekt gemäß Angebot / Projektvertrag).

(2) Die Laufzeit dieses Vertrages entspricht der Laufzeit des Hauptvertrages.

§ 2 Art, Umfang und Zweck der Verarbeitung

Art der Verarbeitung: Erhebung, Speicherung, Anpassung, Auslesen, Abfrage, Verwendung, Übermittlung, Löschung im Rahmen der beauftragten Leistung (insbesondere Betrieb von Web-Anwendungen, Datenbanken, KI-/LLM-Systemen, Wartung und Support).

Zweck der Verarbeitung: Erbringung der im Hauptvertrag vereinbarten Leistungen.

§ 3 Art der Daten und Kategorien betroffener Personen

Kategorien personenbezogener Daten (projektabhängig, im Einzelfall zu präzisieren):

- Stammdaten (Name, Anschrift, Kontaktdaten)
- Vertrags- und Nutzungsdaten
- Kommunikationsdaten (E-Mail, Nachrichten)
- Log- und Metadaten
- Inhaltsdaten (Dokumente, Uploads)
- ggf. besondere Kategorien nach Art. 9 DSGVO — nur nach ausdrücklicher schriftlicher Vereinbarung und mit erhöhtem Schutzniveau

Kategorien betroffener Personen: Mitarbeitende, Kunden, Interessenten, Nutzer und weitere Kontakte des Verantwortlichen.

§ 4 Weisungsrecht des Verantwortlichen

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen (Art. 28 Abs. 3 lit. a DSGVO).

(2) Weisungen erfolgen grundsätzlich in Textform. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

(3) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen datenschutzrechtliche Bestimmungen verstößt.

§ 5 Pflichten des Auftragsverarbeiters

- Verarbeitung ausschließlich im Rahmen der Weisungen des Verantwortlichen.
- Verpflichtung aller mit der Datenverarbeitung befassten Personen zur Vertraulichkeit (Art. 28 Abs. 3 lit. b DSGVO); bei Berufsgeheimnisträgern ergänzend nach § 203 Abs. 4 Satz 2 StGB.
- Umsetzung angemessener technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO (Anlage 1).
- Unterstützung des Verantwortlichen bei der Wahrung der Betroffenenrechte (Art. 12–22 DSGVO).
- Unterstützung bei Datenschutz-Folgenabschätzungen (Art. 35/36 DSGVO).
- Unverzügliche Meldung von Datenschutzverletzungen an den Verantwortlichen, spätestens innerhalb von 24 Stunden nach Kenntniserlangung, mit den in Art. 33 Abs. 3 DSGVO genannten Informationen.
- Führung eines Verzeichnisses aller Kategorien von Verarbeitungstätigkeiten (Art. 30 Abs. 2 DSGVO).

§ 6 Sub-Auftragsverarbeiter

(1) Der Verantwortliche stimmt dem Einsatz der in **Anlage 2** aufgeführten Sub-Auftragsverarbeiter zu (allgemeine schriftliche Genehmigung nach Art. 28 Abs. 2 Satz 2 DSGVO).

(2) Beabsichtigte Änderungen (Hinzuziehung / Austausch) werden dem Verantwortlichen mit einer Vorlauffrist von mindestens 30 Tagen in Textform mitgeteilt. Der Verantwortliche kann innerhalb dieser Frist aus wichtigem Grund widersprechen.

(3) Der Auftragsverarbeiter schließt mit jedem Sub-Auftragsverarbeiter einen Vertrag, der ihm im Wesentlichen die gleichen Pflichten auferlegt wie dieser AVV.

§ 7 Drittlandübermittlung

Eine Übermittlung personenbezogener Daten in ein Drittland erfolgt nur auf Grundlage eines Angemessenheitsbeschlusses (Art. 45 DSGVO) oder unter Einsatz geeigneter Garantien (insbesondere Standardvertragsklauseln nach Art. 46 Abs. 2 lit. c DSGVO). Bei US-Anbietern wird zusätzlich der EU-US Data Privacy Framework berücksichtigt.

§ 8 Kontroll- und Auskunftsrechte

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anfrage alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten erforderlich sind.

(2) Der Verantwortliche ist berechtigt, sich vor Verarbeitungsbeginn und danach regelmäßig – in der Regel einmal jährlich, im Anlassfall auch häufiger – von der Einhaltung der technischen und organisatorischen Maßnahmen zu überzeugen. Prüfungen erfolgen mit angemessener Vorlauffrist, während der Geschäftszeiten und ohne Störung des Betriebsablaufs. Der Nachweis kann auch durch aktuelle Testate, Zertifizierungen oder Prüfberichte erfolgen.

§ 9 Löschung und Rückgabe

Nach Beendigung des Hauptvertrages löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Zusammenhang mit der Verarbeitung verarbeiteten personenbezogenen Daten oder gibt sie zurück. Bestehen gesetzliche Aufbewahrungspflichten, bleibt die Verarbeitung

insoweit eingeschränkt bestehen. Die Löschung wird auf Verlangen in Textform bestätigt.

§ 10 Haftung

Für die Haftung der Parteien gelten Art. 82 DSGVO sowie die Regelungen des Hauptvertrages. Eine über den Hauptvertrag hinausgehende Haftung wird durch diesen AVV nicht begründet.

§ 11 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieses Vertrages bedürfen der Textform.

(2) Sollten einzelne Bestimmungen unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

(3) Es gilt deutsches Recht. Gerichtsstand ist Wiesbaden, sofern der Verantwortliche Kaufmann ist.

Anlage 1 — Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Vertraulichkeit

- Zutrittskontrolle: Büro in verschlossener Villa, Alarm- und Schließanlage.
- Zugangskontrolle: Benutzerkonten mit starken Passwörtern, 2-Faktor-Authentisierung für Admin-Systeme, Bildschirmsperre.
- Zugriffskontrolle: Rollen- und Rechtekonzept (Need-to-know), Trennung von Entwicklungs- und Produktivumgebungen.
- Trennungskontrolle: Mandantenfähige Datenhaltung; Kundendaten werden nicht vermischt.
- Pseudonymisierung / Anonymisierung, wo technisch möglich.

Integrität

- Weitergabekontrolle: Verschlüsselte Übertragung (TLS 1.2+), verschlüsselte VPN-Verbindungen für Wartungszugriffe.
- Eingabekontrolle: Protokollierung wesentlicher Verarbeitungsvorgänge in Admin-Systemen.

Verfügbarkeit und Belastbarkeit

- Regelmäßige Backups, geo-redundante Ablage in EU-Rechenzentren.
- Monitoring, USV bei kritischen on-premise-Systemen.
- Dokumentierter Wiederanlaufplan.

Verfahren zur Überprüfung und Bewertung

- Regelmäßige Überprüfung der TOM, mindestens jährlich.
- Datenschutz-Management: interne Richtlinien, Verpflichtung auf Vertraulichkeit, ggf. § 203 StGB.
- Vorfall-Reaktions-Prozess mit definierten Meldekettten.

Anlage 2 — Zugelassene Sub-Auftragsverarbeiter

- **Kinsta Inc.**, 8605 Santa Monica Blvd #92581, West Hollywood, CA 90069, USA — Hosting/CDN für ki.stadtbewohner.com. Serverstandort: Frankfurt am Main (Google Cloud EU). Rechtsgrundlage Drittland: EU-US Data Privacy Framework und Standardvertragsklauseln.
- **Supabase, Inc.**, 970 Toa Payoh North #07-04, Singapur — Datenbank, Authentifizierung, Formular- und Chat-Speicherung. Verwendete Region: Europäische Union (Frankfurt).

- Weitere projektspezifische Sub-Auftragsverarbeiter (Zahlungsdienstleister, E-Mail-Versand, Analytics etc.) werden ausschließlich nach vorheriger Ergänzung dieser Liste und Freigabe durch den Verantwortlichen eingesetzt.

Unterschriften

Ort, Datum: _____

Verantwortlicher

Björn Becker, Stadtbewohner Webdesign (Auftragsverarbeiter)

Stadtbewohner Webdesign | Björn Becker · Aarstraße 222, 65232 Taunusstein-Wehen · design@stadtbewohner.com ·
ki.stadtbewohner.com