

# Vertrag zur Auftragsverarbeitung

gemäß Art. 28 DSGVO

Hosting-Dienstleistungen – Allgemeine Vorlage

---

zwischen

**den jeweiligen Kunden (Auftraggeber)**

– nachfolgend „Auftraggeber“ –

und

**kreadiv – Florian Wenzel**

Josef-Lang-Str. 5, 81245 München

– nachfolgend „Auftragnehmer“ –

## § 1 Gegenstand und Dauer der Verarbeitung

(1) Der Auftragnehmer erbringt für den Auftraggeber Hosting-Dienstleistungen – Allgemeine Vorlage auf Basis eines Managed Servers bei der Hetzner Online GmbH. Der Gegenstand der Auftragsverarbeitung umfasst insbesondere:

- Bereitstellung und Betrieb von Webhosting-Infrastruktur (Webpace, Datenbanken, E-Mail)
- Technische Administration und Wartung des Servers
- Durchführung von Datensicherungen (Backups)
- Bereitstellung von SSL/TLS-Zertifikaten
- DNS-Verwaltung

(2) Die Dauer der Verarbeitung entspricht der Laufzeit des zwischen den Parteien bestehenden Hosting-Vertrags. Dieser Vertrag endet automatisch mit Beendigung des zugrunde liegenden Hosting-Vertrags.

## § 2 Art und Zweck der Verarbeitung

Die Verarbeitung personenbezogener Daten durch den Auftragnehmer erfolgt im Rahmen der Bereitstellung von Webhosting-Dienstleistungen. Die Art der Verarbeitung umfasst das Erheben, Speichern, Ändern, Auslesen, Abfragen, die Verwendung, Offenlegung durch Übermittlung, Einschränkung und Löschung von Daten auf dem bereitgestellten Server.

Der Zweck der Verarbeitung ergibt sich aus dem jeweiligen Hosting-Vertrag und den vom Auftraggeber auf dem Server betriebenen Anwendungen (Websites, Onlineshops, E-Mail-Dienste etc.).

## § 3 Kategorien betroffener Personen und personenbezogener Daten

**Kategorien betroffener Personen:** Die Kategorien betroffener Personen ergeben sich aus der jeweiligen Nutzung durch den Auftraggeber und können insbesondere umfassen: Kunden, Interessenten, Beschäftigte, Lieferanten und Geschäftspartner des Auftraggebers sowie Nutzer der vom Auftraggeber betriebenen Websites und Dienste.

**Kategorien personenbezogener Daten:** Die Kategorien personenbezogener Daten ergeben sich aus der jeweiligen Nutzung durch den Auftraggeber und können insbesondere umfassen: Name, Kontaktdaten (E-Mail, Telefon, Anschrift), Nutzungsdaten (IP-Adressen, Zugriffszeiten), Bestelldaten, Zahlungsdaten, Inhaltsdaten (Formulareinträge, hochgeladene Dateien) sowie Kommunikationsinhalte (E-Mails).

## § 4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, es sei denn, er ist nach Unionsrecht oder dem Recht der Mitgliedstaaten, dem er unterliegt, zur Verarbeitung verpflichtet.

(2) Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung personenbezogener Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(3) Der Auftragnehmer ergreift alle gemäß Art. 32 DSGVO erforderlichen Maßnahmen. Die technischen und organisatorischen Maßnahmen (TOM) sind in Anlage 1 beschrieben.

(4) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung bei der Erfüllung der Betroffenenrechte gemäß Kapitel III DSGVO.

(5) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in Art. 32–36 DSGVO genannten Pflichten (Sicherheit, Meldepflichten, Datenschutz-Folgenabschätzung, vorherige Konsultation).

(6) Der Auftragnehmer löscht nach Beendigung der Auftragsverarbeitung alle personenbezogenen Daten und deren Kopien, sofern nicht eine gesetzliche Aufbewahrungspflicht besteht. Die Löschung wird dem Auftraggeber schriftlich bestätigt.

(7) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung und ermöglicht und trägt zu Überprüfungen – einschließlich Inspektionen – bei, die vom Auftraggeber oder einem von diesem beauftragten Prüfer durchgeführt werden.

## § 5 Pflichten des Auftraggebers

(1) Der Auftraggeber ist für die Rechtmäßigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen allein verantwortlich (Art. 4 Nr. 7 DSGVO).

(2) Der Auftraggeber ist für die Sicherheit der von ihm auf dem Server installierten und betriebenen Software selbst verantwortlich. Dies umfasst sowohl Standardsoftware (Content-Management-Systeme, Plugins, Themes, Frameworks) als auch selbst entwickelte oder in Auftrag gegebene individuelle Software (Webanwendungen, Skripte, APIs, Microservices, Cronjobs etc.). **Dies umfasst insbesondere:**

- a) **Aktualisierungspflicht:** Der Auftraggeber verpflichtet sich, die von ihm eingesetzte Software stets aktuell und sicher zu halten. Bei Standardsoftware (CMS-Systeme, Plugins, Themes, Frameworks und Erweiterungen) sind verfügbare Sicherheitsupdates zeitnah – spätestens innerhalb von 14 Tagen nach Veröffentlichung – einzuspielen. Bei selbst entwickelter oder individuell beauftragter Software trägt der Auftraggeber die Verantwortung dafür, dass diese nach dem Stand der Technik entwickelt wird, bekannte Sicherheitsstandards einhält (z. B. OWASP Top 10) und regelmäßig auf Schwachstellen geprüft wird.
- b) **Sicherheitsverantwortung:** Der Auftraggeber trägt die volle Verantwortung für Sicherheitslücken, die durch veraltete, fehlerhafte, unsichere oder nicht ordnungsgemäß konfigurierte Software entstehen – unabhängig davon, ob es sich um Standardsoftware oder selbst entwickelte bzw. individuell beauftragte Software handelt.
- c) **Schadensfreistellung:** Der Auftraggeber stellt den Auftragnehmer von allen Ansprüchen, Schäden, Kosten und Aufwendungen frei, die dem Auftragnehmer durch Sicherheitslücken in der vom Auftraggeber installierten oder betriebenen Software entstehen. Dies gilt insbesondere für Schäden an Drittsystemen, Kosten für die Bereinigung kompromittierter Systeme, behördliche Bußgelder sowie Reputationsschäden.
- d) **Meldepflicht:** Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn ihm Sicherheitslücken oder kompromittierte Anwendungen auf seinem Webspace bekannt werden.

(3) Der Auftraggeber erteilt alle Weisungen, die die Verarbeitung personenbezogener Daten betreffen, schriftlich oder in Textform (z. B. E-Mail).

(4) Der Auftraggeber benennt einen Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

## § 6 Notfall- und Sicherheitsmaßnahmen des Auftragnehmers

(1) Der Auftragnehmer ist berechtigt, bei akuter Gefährdung der Serversicherheit oder der Sicherheit Dritter durch vom Auftraggeber betriebene Software unverzüglich folgende Maßnahmen zu ergreifen:

- Temporäre Sperrung oder Deaktivierung betroffener Websites, Anwendungen oder Dienste
- Entzug von Dateiberechtigungen oder Zugriff auf kompromittierte Verzeichnisse
- Isolierung betroffener Bereiche vom Netzwerk
- Temporäre Änderung von Zugangsdaten

(2) Der Auftragnehmer informiert den Auftraggeber unverzüglich, spätestens jedoch innerhalb von 24 Stunden, über ergriffene Notfallmaßnahmen und deren Gründe.

(3) Der Auftragnehmer haftet nicht für Schäden, die dem Auftraggeber durch berechtigte Notfallmaßnahmen gemäß Abs. 1 entstehen.

## § 7 Meldepflichten bei Datenschutzverstößen

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der Meldepflichten gemäß Art. 33 und 34 DSGVO.

(2) Der Auftragnehmer informiert den Auftraggeber unverzüglich, spätestens innerhalb von 48 Stunden, nachdem ihm eine Verletzung des Schutzes personenbezogener Daten bekannt geworden ist. Die Meldung enthält mindestens:

- Beschreibung der Art der Verletzung
- Bezeichnung der Kategorien und ungefähre Anzahl der betroffenen Personen und Datensätze
- Beschreibung der wahrscheinlichen Folgen der Verletzung
- Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen

## § 8 Unterauftragnehmer

(1) Der Auftraggeber stimmt dem Einsatz folgender Unterauftragnehmer zu:

Unterauftragnehmer	Leistung	Standort
Hetzner Online GmbH	Managed Server, Rechenzentrumsbetrieb, Netzwerkinfrastruktur	Deutschland

(2) Der Auftragnehmer informiert den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung von Unterauftragnehmern. Der Auftraggeber kann gegen solche Änderungen Einspruch erheben.

(3) Der Auftragnehmer stellt durch vertragliche Vereinbarungen sicher, dass die Unterauftragnehmer dieselben Datenschutzverpflichtungen einhalten wie in diesem Vertrag festgelegt.

## § 9 Haftung und Haftungsbegrenzung

(1) Die Parteien haften einander nach den gesetzlichen Bestimmungen, soweit in diesem Vertrag nichts anderes geregelt ist.

(2) Der Auftragnehmer haftet nicht für Schäden, die durch Sicherheitslücken, Fehlfunktionen oder unsachgemäße Konfiguration von Software entstehen, die der Auftraggeber eigenständig auf dem bereitgestellten Webspace installiert, entwickelt oder betreibt. Dies gilt gleichermaßen für Standardsoftware (CMS, Plugins, Frameworks) wie für selbst entwickelte oder individuell beauftragte Software und umfasst insbesondere:

- Schäden durch veraltete CMS-Versionen, Plugins, Themes, Frameworks oder sonstige Erweiterungen sowie durch Sicherheitslücken in selbst entwickelter oder individuell beauftragter Software (z. B. SQL-Injection, Cross-Site-Scripting, fehlerhafte Authentifizierung, unsichere API-Endpunkte)
- Schäden durch Malware oder Schadcode, der über unsichere Anwendungen des Auftraggebers eingeschleust wird
- Datenverluste, die auf fehlerhafte Skripte, selbst entwickelten Code oder Datenbankkonfigurationen des Auftraggebers zurückzuführen sind
- Schäden an Drittsystemen oder Drittdateien, die durch kompromittierte Anwendungen des Auftraggebers verursacht werden

(3) Die Haftung des Auftragnehmers für leichte Fahrlässigkeit ist auf die Verletzung vertragswesentlicher Pflichten (Kardinalpflichten) beschränkt und wird der Höhe nach auf den vorhersehbaren, vertragstypischen Schaden begrenzt, maximal jedoch auf die jährliche Nettoumsatzsumme.

(4) Die vorstehenden Haftungsbeschränkungen gelten nicht bei Vorsatz, grober Fahrlässigkeit, Verletzung des Lebens, des Körpers oder der Gesundheit sowie bei zwingender gesetzlicher Haftung (z. B. nach dem Produkthaftungsgesetz).

## § 10 Laufzeit und Kündigung

(1) Dieser Vertrag tritt mit Unterzeichnung durch beide Parteien in Kraft und wird auf unbestimmte Zeit geschlossen. Er endet automatisch mit der Beendigung des zugrunde liegenden Hosting-Vertrags.

(2) Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt. Ein wichtiger Grund liegt insbesondere vor, wenn:

- der Auftraggeber wiederholt und trotz Mahnung gegen seine Pflichten aus § 5 (insbesondere die Aktualisierungspflicht) verstößt
- die Fortsetzung des Vertrags aufgrund einer wesentlichen Änderung der datenschutzrechtlichen Lage unzumutbar ist
- der Auftragnehmer wesentliche Bestimmungen dieses Vertrags verletzt

## § 11 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieses Vertrags bedürfen der Schriftform. Dies gilt auch für die Änderung dieser Schriftformklausel.

(2) Sollte eine Bestimmung dieses Vertrags unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen davon unberührt. Die Parteien verpflichten sich, die unwirksame Bestimmung durch eine wirksame Bestimmung zu ersetzen, die dem wirtschaftlichen Zweck der unwirksamen Bestimmung am nächsten kommt.

(3) Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist München.

(4) Dieser Vertrag wird in zwei gleichlautenden Exemplaren ausgefertigt, von denen jede Partei eines erhält.

## § 12 Geltung und Inkrafttreten

Dieser Vertrag zur Auftragsverarbeitung ist integraler Bestandteil der Allgemeinen Geschäftsbedingungen für Webhosting und Domains der Firma kreadiv (§ 1 Abs. 6 AGB) und gilt mit Abschluss eines Hosting-Vertrags als vereinbart. Eine gesonderte Unterzeichnung ist nicht erforderlich.

### **Auftragnehmer:**

kreadiv – Florian Wenzel  
Josef-Lang-Str. 5, 81245 München  
München, Februar 2026

## Anlage 1: Technische und organisatorische Maßnahmen (TOM)

Die folgenden technischen und organisatorischen Maßnahmen werden vom Auftragnehmer gemäß Art. 32 DSGVO umgesetzt und sind Bestandteil dieses Vertrags:

Maßnahme	Beschreibung
<b>Zutrittskontrolle</b>	Serverstandort: Hetzner-Rechenzentrum (ISO 27001 zertifiziert) in Deutschland. Zugang nur durch autorisiertes Hetzner-Personal. Auftragnehmer hat keinen physischen Zugang zu den Servern.
<b>Zugangskontrolle</b>	SSH-Zugang ausschließlich über Key-Authentifizierung. Root-Zugang deaktiviert. Individuelle Benutzerkonten mit starken Passwörtern. Zwei-Faktor-Authentifizierung für Verwaltungszugang (Hetzner konsoleH).
<b>Zugriffskontrolle</b>	Berechtigungskonzept nach dem Prinzip der minimalen Rechte. Webhosting-Kunden haben nur Zugriff auf ihren eigenen Webspace. Trennung der Kundendaten durch separate Benutzerkonten und Datenbanken.
<b>Weitergabekontrolle</b>	Verschlüsselte Datenübertragung via TLS/SSL. SFTP/SSH für Dateitransfer. Keine unverschlüsselte Übertragung personenbezogener Daten.
<b>Eingabekontrolle</b>	Protokollierung von Zugriffen und Änderungen auf Serverebene. Logfiles werden nach 30 Tagen gelöscht.
<b>Auftragskontrolle</b>	Verarbeitung personenbezogener Daten ausschließlich gemäß den Weisungen des Auftraggebers. Keine Weitergabe an Dritte ohne Genehmigung.
<b>Verfügbarkeitskontrolle</b>	Tägliche Backups. Redundante Speichersysteme (RAID). Unterbrechungsfreie Stromversorgung (USV) im Rechenzentrum. Notfallwiederherstellungsplan vorhanden.
<b>Trennungsgebot</b>	Logische Trennung der Kundendaten durch separate Datenbanken, FTP-Konten und Webspaces. Mandantenfähige Serverkonfiguration.

**Hinweis:** Die physische Sicherheit des Rechenzentrums (Zutrittskontrolle, Brandschutz, Klimatisierung, Stromversorgung) obliegt dem Unterauftragnehmer Hetzner Online GmbH, der hierfür gemäß seinem eigenen AV-Vertrag und seiner ISO-27001-Zertifizierung verantwortlich ist.

Die Maßnahmen werden regelmäßig auf ihre Wirksamkeit überprüft und bei Bedarf angepasst. Änderungen werden dem Auftraggeber mitgeteilt.

## Anlage 2: Verantwortlichkeiten des Auftraggebers für Software-Sicherheit

Diese Anlage konkretisiert die in § 5 Abs. 2 genannten Pflichten des Auftraggebers und dient der klaren Abgrenzung der Verantwortlichkeiten:

### 1. Verantwortungsbereich des Auftraggebers

Der Auftraggeber ist allein verantwortlich für:

- Auswahl, Installation, Konfiguration und Betrieb aller von ihm auf dem Webservice eingesetzten Softwarekomponenten
- Regelmäßige Prüfung auf verfügbare Sicherheitsupdates und deren zeitnahe Installation
- Sichere Konfiguration der eingesetzten CMS-Systeme (z. B. Contao, WordPress, Kirby, Shopify-Anbindungen) sowie sicherer Betrieb selbst entwickelter oder individuell beauftragter Webanwendungen
- Sichere Verwaltung von Zugangsdaten (FTP, SSH, Datenbank, CMS-Backend)
- Regelmäßige Prüfung der Webseiten-Inhalte auf rechtswidrige oder schadhafte Inhalte
- Einhaltung des Datenschutzes in den vom Auftraggeber betriebenen Anwendungen (z. B. Cookie-Consent, Datenschutzerklärung, Formularverarbeitung)
- Bei selbst entwickelter Software: Einhaltung anerkannter Sicherheitsstandards (insbesondere OWASP Top 10), sichere Programmierung (Eingabevalidierung, Prepared Statements, sichere Session-Verwaltung), regelmäßige Code-Reviews und Schwachstellenprüfungen

### 2. Verantwortungsbereich des Auftragnehmers

Der Auftragnehmer ist verantwortlich für:

- Betrieb und Wartung der Serverinfrastruktur (Betriebssystem, Webserver, PHP, Datenbank-Server)
- Regelmäßige Aktualisierung der serverseitigen Software (OS-Updates, PHP-Versionen, Apache/nginx, MariaDB/MySQL)
- Durchführung und Überwachung von Backups
- Grundlegende Absicherung des Servers (Firewall, Fail2Ban, SSH-Härtung)
- Überwachung der Serververfügbarkeit und -leistung

### 3. Eskalationsverfahren bei Sicherheitsvorfällen

Im Falle eines Sicherheitsvorfalls gilt folgendes Verfahren:

Stufe	Maßnahme	Frist
1	Erkennung und Bewertung des Vorfalls durch den Auftragnehmer	Unverzüglich
2	Information des Auftraggebers per E-Mail	Innerhalb von 24 Stunden

3	Ergreifung von Sofortmaßnahmen gem. § 6	Unverzüglich bei akuter Gefahr
4	Behebung durch den Auftraggeber (Software-Update, Bereinigung)	Innerhalb von 72 Stunden
5	Freischaltung nach Bestätigung der Behebung	Nach Prüfung

Verstreicht die Frist in Stufe 4 ohne Reaktion des Auftraggebers, behält sich der Auftragnehmer das Recht vor, die betroffenen Dienste bis zur Behebung gesperrt zu lassen. **Bei wiederholten Sicherheitsvorfällen behält sich der Auftragnehmer das Recht zur außerordentlichen Kündigung gemäß § 10 Abs. 2 vor.**

#### 4. Haftungsausschluss bei Kundensoftware

Zur Klarstellung: Der Auftragnehmer übernimmt keinerlei Haftung für:

- Datenverluste oder Datenschutzverstöße, die durch unsichere Anwendungen des Auftraggebers verursacht werden
- Schäden an Dritten (z. B. anderen Kunden auf dem Server), die durch kompromittierte Anwendungen des Auftraggebers entstehen
- Bußgelder oder Abmahnkosten, die auf die Nichtbeachtung der Aktualisierungspflicht oder auf Sicherheitsmängel in selbst entwickelter Software des Auftraggebers zurückzuführen sind
- Umsatzeinbußen oder Betriebsunterbrechungen, die durch Sicherheitsmaßnahmen gemäß § 6 verursacht werden

**Stand:** Februar 2026