

Vertrag zur Auftragsverarbeitung

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO) – für Wartungs- und Betreuungsverträge · Stand: Oktober 2026

zwischen

Verantwortlicher
(„Auftraggeber“)

Firma: _____

Anschrift: _____

vertreten durch: _____

und Auftragsverarbeiter
(„Auftragnehmer“)

Oleksiy Ostapenko – Webdesign & IT-Lösungen
Edisonstraße 44, 65199 Wiesbaden
E-Mail: info@webdesign-experte-wiesbaden.de

§ 1 Gegenstand und Dauer

(1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen auf Grundlage des Hauptvertrags (Angebot vom _____ bzw. Wartungsvertrag, Paket: _____). Dabei kann der Auftragnehmer Zugriff auf personenbezogene Daten erhalten, für die der Auftraggeber Verantwortlicher ist. Gegenstand, Art und Zweck der Verarbeitung, die Art der Daten und die Kategorien betroffener Personen ergeben sich aus **Anlage 1**.

(2) Dieser Vertrag gilt für die Dauer des Hauptvertrags und endet mit ihm, ohne dass es einer gesonderten Kündigung bedarf. Pflichten, die über das Vertragsende hinausreichen (insbesondere § 10 und § 4 Abs. 1), bleiben bestehen.

§ 2 Weisungsgebundenheit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen des Hauptvertrags und nach dokumentierter Weisung des Auftraggebers, es sei denn, er ist durch das Recht der Union oder eines Mitgliedstaats zur Verarbeitung verpflichtet; in diesem Fall teilt er dem Auftraggeber diese Anforderungen vorher mit, sofern das Recht dies nicht verbietet.

(2) Weisungen erteilt der Auftraggeber in Textform (z. B. per E-Mail). Mündliche Weisungen bestätigt er unverzüglich in Textform.

(3) Ist der Auftragnehmer der Ansicht, dass eine Weisung gegen Datenschutzvorschriften verstößt, weist er den Auftraggeber unverzüglich darauf hin. Er darf die Ausführung aussetzen, bis der Auftraggeber die Weisung bestätigt oder ändert.

§ 3 Ort der Verarbeitung

Die Verarbeitung findet ausschließlich in der Europäischen Union statt. Eine Übermittlung in ein Drittland erfolgt nur mit vorheriger Zustimmung des Auftraggebers in Textform und nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

§ 4 Vertraulichkeit

(1) Der Auftragnehmer wahrt die Vertraulichkeit der personenbezogenen Daten, auch nach Beendigung des Vertrags.

(2) Setzt der Auftragnehmer Personen zur Verarbeitung ein, verpflichtet er sie vorher zur Vertraulichkeit, sofern sie nicht einer gesetzlichen Verschwiegenheitspflicht unterliegen. Der Auftragnehmer ist derzeit als Einzelunternehmer ohne Beschäftigte tätig.

§ 5 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer trifft die in **Anlage 2** beschriebenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO und hält sie während der Vertragsdauer ein.

(2) Die Maßnahmen dürfen an den technischen Fortschritt angepasst werden, sofern das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen teilt der Auftragnehmer dem Auftraggeber in Textform mit.

§ 6 Unterauftragsverarbeiter

(1) Der Auftraggeber erteilt die allgemeine Genehmigung, Unterauftragsverarbeiter einzusetzen. Die bei Vertragsschluss eingesetzten bzw. vorgesehenen Unterauftragsverarbeiter sind in **Anlage 3** aufgeführt und gelten als genehmigt.

(2) Über jede beabsichtigte Hinzuziehung oder Ersetzung informiert der Auftragnehmer den Auftraggeber mindestens 14 Tage vorher in Textform. Der Auftraggeber kann innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund widersprechen. Kommt keine Einigung zustande, können beide Parteien den Hauptvertrag hinsichtlich der betroffenen Leistung kündigen.

(3) Der Auftragnehmer verpflichtet Unterauftragsverarbeiter vertraglich auf dieselben Datenschutzpflichten, wie sie in diesem Vertrag festgelegt sind (Art. 28 Abs. 4 DSGVO).

(4) Keine Unterauftragsverarbeitung sind Nebenleistungen, die der Auftragnehmer bei Dritten in Anspruch nimmt, ohne dass diese Zugriff auf die personenbezogenen Daten des Auftraggebers erhalten (z. B. Telekommunikation). Das Hosting der Website des Auftraggebers ist kein Unterauftrag des Auftragnehmers, wenn der Auftraggeber den Hostingvertrag selbst abgeschlossen hat.

§ 7 Rechte betroffener Personen

Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Beantwortung von Anträgen betroffener Personen (Art. 12–22 DSGVO). Wendet sich eine betroffene Person direkt an den Auftragnehmer, leitet er die Anfrage unverzüglich an den Auftraggeber weiter.

§ 8 Unterstützungs- und Meldepflichten

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der Pflichten aus Art. 32–36 DSGVO (Sicherheit, Meldung von Verletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation).

(2) Verletzungen des Schutzes personenbezogener Daten meldet der Auftragnehmer dem Auftraggeber unverzüglich, möglichst innerhalb von 24 Stunden nach Kenntnis, mit den ihm vorliegenden Angaben nach Art. 33 Abs. 3 DSGVO. Er ergreift unverzüglich die erforderlichen Maßnahmen, um die Verletzung einzudämmen.

§ 9 Nachweise und Kontrollen

(1) Der Auftragnehmer stellt dem Auftraggeber auf Anfrage alle erforderlichen Informationen zum Nachweis der Einhaltung dieses Vertrags zur Verfügung.

(2) Der Auftraggeber oder ein von ihm beauftragter, zur Verschwiegenheit verpflichteter Prüfer kann die Einhaltung nach vorheriger Ankündigung mit angemessener Frist (in der Regel 14 Tage) während der üblichen Geschäftszeiten prüfen. Der Auftragnehmer kann den damit verbundenen Aufwand angemessen in Rechnung stellen, sofern die Prüfung keinen Verstoß ergibt.

§ 10 Löschung und Rückgabe

Nach Ende der Leistungen löscht der Auftragnehmer nach Wahl des Auftraggebers alle personenbezogenen Daten oder gibt sie zurück, einschließlich vorhandener Kopien und Datensicherungen, sofern keine gesetzliche Pflicht zur Speicherung besteht. Ohne anderslautende Weisung innerhalb von 14 Tagen nach Vertragsende werden die Daten gelöscht; Datensicherungen spätestens mit Ablauf ihrer regulären Aufbewahrungsfrist. Die Löschung bestätigt der Auftragnehmer auf Anfrage in Textform.

§ 11 Haftung und Schlussbestimmungen

(1) Für die Haftung gilt Art. 82 DSGVO. Im Übrigen gelten die Haftungsregelungen des Hauptvertrags bzw. der AGB des Auftragnehmers.

(2) Änderungen und Ergänzungen bedürfen der Textform. Bei Widersprüchen geht dieser Vertrag den Regelungen des Hauptvertrags zum Datenschutz vor.

(3) Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

(4) Es gilt deutsches Recht.

Ort, Datum

Ort, Datum

Auftraggeber (Name, Unterschrift)

Oleksiy Ostapenko, Auftragnehmer

Alternativ kann dieser Vertrag in elektronischer Form (z. B. durch Bestätigung per E-Mail) geschlossen werden (Art. 28 Abs. 9 DSGVO).

Anlage 1 – Gegenstand der Verarbeitung

Gegenstand und Zweck	Wartung, Pflege und technische Betreuung der Website des Auftraggebers: Updates von Kern, Themes und Plugins, Erstellung und Wiederherstellung von Datensicherungen, Überwachung von Erreichbarkeit und Sicherheit, Fehlerbehebung und kleinere Anpassungen gemäß Hauptvertrag.
Art der Verarbeitung	Speichern (Datensicherungen), Einsehen, Kopieren und Wiederherstellen von Datenbanken und Dateien, Löschen; Zugriff erfolgt im Rahmen von Wartungsarbeiten.
Art der Daten	Daten, die in der Website bzw. ihrer Datenbank gespeichert sind, insbesondere: Kontakt- und Formulardaten (Name, E-Mail, Telefon, Nachrichteninhalte), Benutzerkonten (Benutzername, E-Mail, Passwort-Hashes), Kommentare, ggf. Bestell- und Kundendaten (z. B. bei Online-Shops), technische Protokolldaten (IP-Adressen, Zeitstempel).
Betroffene Personen	Besucher und Nutzer der Website, Interessenten und Kunden des Auftraggebers, Beschäftigte und Redakteure des Auftraggebers.
Besondere Kategorien (Art. 9 DSGVO)	Nicht vorgesehen. Verarbeitet die Website solche Daten, teilt der Auftraggeber dies vor Vertragsschluss mit: _____

Anlage 2 – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Zutrittskontrolle	Arbeitsgeräte befinden sich in privaten, abschließbaren Räumen; Rechenzentren der Unterauftragsverarbeiter mit Zutrittskontrolle (siehe deren Nachweise).
Zugangskontrolle	Geräte mit Festplattenverschlüsselung und Bildschirmsperre; individuelle, starke Passwörter aus einem Passwortmanager; Zwei-Faktor-Authentifizierung, wo angeboten; Server-Zugriff per SSH-Schlüssel.
Zugriffskontrolle	Zugänge nur im für die Wartung erforderlichen Umfang; getrennte Zugänge je Auftraggeber; Zugangsdaten werden nicht an Dritte weitergegeben.
Weitergabekontrolle	Übertragungen ausschließlich verschlüsselt (HTTPS, SFTP/SSH); keine Übermittlung an Dritte außer an Unterauftragsverarbeiter nach Anlage 3; keine Kopien auf unverschlüsselten Datenträgern.
Eingabekontrolle	Dokumentation der Wartungsarbeiten im monatlichen Bericht; Änderungen nachvollziehbar über Zeitpunkt und Art der Arbeit.
Trennungskontrolle	Datensicherungen je Auftraggeber in getrennten Verzeichnissen bzw. Zugängen; Test-Kopien (Staging) getrennt von der Live-Website.
Verfügbarkeit und Belastbarkeit	Regelmäßige Datensicherungen gemäß Paket; Sicherung vor jedem Update; regelmäßige Prüfung der Wiederherstellbarkeit; Überwachung der Erreichbarkeit.
Löschung	Datensicherungen werden nach Ablauf der im Paket vereinbarten Aufbewahrungsdauer automatisch bzw. regelmäßig gelöscht; nach Vertragsende gemäß § 10.
Regelmäßige Überprüfung	Überprüfung der Maßnahmen mindestens jährlich sowie bei wesentlichen Änderungen der Werkzeuge.

Anlage 3 – Unterauftragsverarbeiter

Unternehmen	Leistung	Ort der Verarbeitung
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen	Speicherplatz für Datensicherungen (Storage Box)	Deutschland

Der Hostinganbieter der Website ist Vertragspartner des Auftraggebers und kein Unterauftragsverarbeiter des Auftragnehmers (§ 6 Abs. 4).