

Auftragsverarbeitungsvertrag (AVV)

Fassung Oktober 2026 · in Kraft seit 15. September 2026 · hmaidan.media, Daniel Hmaidan,
Holsteinstraße 2, 35684 Dillenburg

Für jeden Vertrag gilt die Fassung, die bei Vertragsschluss vereinbart oder später in Textform
angenommen wurde. Alle Fassungen: agentur.hmaidan.de/vertrag

1. Gegenstand und Begriffe

1. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers im Sinne des Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, nachfolgend „DSGVO“). Dieser Vertrag regelt die Rechte und Pflichten der Parteien.
2. Verwenden die Parteien den Begriff „Verarbeitung“, gilt die Begriffsbestimmung des Art. 4 Nr. 2 DSGVO.
3. Dieser Vertrag ergänzt den zwischen den Parteien geschlossenen Hauptvertrag über Webdesign-, Hosting- und Zusatzleistungen. Bei Widersprüchen zu datenschutzrechtlichen Fragen geht dieser Vertrag vor.

2. Gegenstand des Auftrags

Gegenstand, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in **Anlage 1** festgelegt.

3. Rechte und Pflichten des Auftraggebers

1. Der Auftraggeber ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Er ist für die Rechtmäßigkeit der Verarbeitung und für die Wahrung der Rechte betroffener Personen verantwortlich.
2. Der Auftraggeber erteilt Weisungen zu Art, Umfang und Verfahren der Verarbeitung. Weisungen erfolgen in **Textform** (zum Beispiel per E-Mail an service@hmaidan.de) und werden vom Auftragnehmer dokumentiert.
3. Der Auftraggeber kann weisungsberechtigte Personen benennen und Änderungen in Textform mitteilen. Ohne eine solche Benennung gilt der im Hauptvertrag genannte Ansprechpartner als weisungsberechtigt.
4. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.
5. Entsteht dem Auftragnehmer durch ergänzende Weisungen ein Mehraufwand, der über den vereinbarten Leistungsumfang hinausgeht, wird dieser nach den im Angebot genannten Sätzen vergütet.
6. Besteht eine Meldepflicht nach Art. 33, 34 DSGVO gegenüber der Aufsichtsbehörde oder betroffenen Personen, ist der Auftraggeber für deren Erfüllung verantwortlich; der Auftragnehmer unterstützt ihn dabei nach Ziffer 4 Abs. 6.

4. Pflichten des Auftragnehmers

1. **Verarbeitung nur nach Weisung.** Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen dieses Vertrages und der Weisungen des Auftraggebers. Hält er eine Weisung für rechtswidrig, teilt er dies unverzüglich mit und darf ihre Ausführung bis zur Klärung aussetzen.
2. **Vertraulichkeit.** Der Auftragnehmer stellt sicher, dass alle zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Diese Verpflichtung besteht auch nach Beendigung des Vertrages fort.
3. **Technische und organisatorische Maßnahmen.** Der Auftragnehmer trifft die nach Art. 32 DSGVO erforderlichen Maßnahmen. Der Stand ist in **Anlage 3** beschrieben. Er darf die Maßnahmen weiterentwickeln, solange das Schutzniveau nicht unterschritten wird; wesentliche Änderungen teilt er in Textform mit.
4. **Trennung.** Die Daten des Auftraggebers werden von Daten anderer Auftraggeber getrennt verarbeitet.
5. **Unterstützung bei Betroffenenrechten.** Wenden sich betroffene Personen mit einem Auskunfts-, Berichtigungs-, Lösch-, Einschränkung-, Widerspruchs- oder Datenübertragbarkeitsverlangen an den Auftragnehmer, leitet er das Verlangen unverzüglich an den Auftraggeber weiter und beantwortet es nicht selbst. Er unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung nachzukommen.
6. **Unterstützung bei Sicherheit und Meldungen.** Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO, insbesondere bei der Sicherheit der Verarbeitung, bei Meldungen von Verletzungen des Schutzes personenbezogener Daten und bei einer Datenschutz-Folgenabschätzung.
7. **Meldung von Verletzungen.** Wird dem Auftragnehmer eine Verletzung des Schutzes personenbezogener Daten bekannt, meldet er sie dem Auftraggeber unverzüglich, spätestens innerhalb von **24 Stunden** nach Kenntnis, in Textform. Die Meldung enthält, soweit bekannt: Art der Verletzung, betroffene Datenkategorien, ungefähre Zahl der betroffenen Personen und Datensätze, wahrscheinliche Folgen sowie ergriffene und vorgeschlagene Maßnahmen. Fehlende Angaben werden unverzüglich nachgereicht.
8. **Verzeichnis.** Der Auftragnehmer führt ein Verzeichnis aller Kategorien von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO und legt es dem Auftraggeber auf Anforderung vor.
9. **Nachweise und Überprüfungen.** Der Auftragnehmer stellt dem Auftraggeber alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO erforderlich sind, und ermöglicht Überprüfungen. Der Nachweis kann durch Selbstauskunft, aktuelle Testate, Zertifikate oder Berichte unabhängiger Stellen geführt werden. Reicht dies nicht aus, kann der Auftraggeber nach Ankündigung mit einer Frist von vier Wochen während der üblichen Geschäftszeiten eine Überprüfung vornehmen oder durch einen zur Verschwiegenheit verpflichteten Prüfer vornehmen lassen, der

kein Wettbewerber des Auftragnehmers sein darf. Der Auftragnehmer kann für den Aufwand einer Vor-Ort-Prüfung eine angemessene Vergütung verlangen.

10. **Löschung und Rückgabe.** Nach Beendigung der Verarbeitung löscht der Auftragnehmer alle personenbezogenen Daten oder gibt sie zurück — **nach Wahl des Auftraggebers**, die dieser bis spätestens einen Monat nach Vertragsende in Textform mitteilt. Ohne Mitteilung wird gelöscht. Ausgenommen sind Daten, für die eine gesetzliche Aufbewahrungspflicht besteht; diese werden gesperrt und nach Ablauf der Frist gelöscht. Die Löschung wird dokumentiert und auf Anforderung bestätigt.

5. Unterauftragnehmer

1. Der Auftraggeber erteilt seine **allgemeine Genehmigung** zur Beauftragung der in **Anlage 2** genannten Unterauftragnehmer.
2. Beabsichtigt der Auftragnehmer, einen weiteren Unterauftragnehmer hinzuzuziehen oder einen bestehenden zu ersetzen, teilt er dies dem Auftraggeber **mindestens vier Wochen vorher** in Textform mit. Der Auftraggeber kann innerhalb von **zwei Wochen** nach Zugang aus einem wichtigen datenschutzrechtlichen Grund widersprechen. Widerspricht er, kann der Auftragnehmer die betroffene Leistung mit einer Frist von einem Monat kündigen, wenn sie ohne den Unterauftragnehmer nicht zu erbringen ist.
3. Der Auftragnehmer verpflichtet jeden Unterauftragnehmer auf dieselben Datenschutzpflichten, die in diesem Vertrag vereinbart sind, und bleibt dem Auftraggeber gegenüber verantwortlich.
4. Keine Unterauftragsverarbeitung sind Nebenleistungen wie Telekommunikation, Post- und Transportdienste, Wartung von Endgeräten oder die Entsorgung von Datenträgern. Für sie sorgt der Auftragnehmer für angemessenen Schutz.

6. Verarbeitung außerhalb der EU

1. Die Verarbeitung findet in der Regel in einem Mitgliedstaat der Europäischen Union oder des Europäischen Wirtschaftsraums statt.
2. Eine Verarbeitung in einem Drittland ist nur zulässig, wenn die Voraussetzungen der Art. 44 bis 49 DSGVO erfüllt sind — insbesondere bei einem Angemessenheitsbeschluss der Europäischen Kommission oder bei Vereinbarung der Standardvertragsklauseln nebst erforderlichen zusätzlichen Maßnahmen. Betroffene Unterauftragnehmer und die jeweilige Grundlage sind in **Anlage 2** gekennzeichnet.

7. Ansprechpartner für den Datenschutz

1. Der Auftragnehmer ist ein Einzelunternehmen. Die Voraussetzungen für die Benennung eines Datenschutzbeauftragten nach Art. 37 DSGVO und § 38 BDSG liegen nicht vor; ein Datenschutzbeauftragter ist daher nicht bestellt.
2. Ansprechpartner für alle Fragen des Datenschutzes ist die in **Anlage 4** genannte Person.
3. Ändern sich die Voraussetzungen, benennt der Auftragnehmer einen Datenschutzbeauftragten und teilt dessen Kontaktdaten unverzüglich mit.

8. Laufzeit

1. Dieser Vertrag beginnt mit dem Hauptvertrag und **endet mit ihm**. Eine gesonderte Kündigung ist ausgeschlossen, solange der Auftragnehmer für den Auftraggeber personenbezogene Daten verarbeitet.
2. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt. Ein wichtiger Grund liegt für den Auftraggeber insbesondere vor, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag trotz Fristsetzung nicht nachkommt.

9. Haftung

Für die Haftung gilt Art. 82 DSGVO. Im Übrigen gelten die Haftungsregelungen des Hauptvertrages.

10. Schlussbestimmungen

1. Änderungen und Ergänzungen dieses Vertrages bedürfen der **Textform**. Das gilt auch für die Aufhebung dieses Formerfordernisses.
2. Ist eine Bestimmung unwirksam, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien ersetzen die unwirksame Bestimmung durch eine wirksame, die dem verfolgten Zweck am nächsten kommt.
3. Es gilt das Recht der Bundesrepublik Deutschland.

Anlage 1: Gegenstand des Auftrags

Kategorie personenbezogener Daten	Zweck der Verarbeitung	Betroffene Personen
Stammdaten (Name, Anschrift, Funktion)	Erbringung der vereinbarten Leistungen, Identifikation, Vertragsabwicklung	Kunden des Auftraggebers und deren Ansprechpartner
Kommunikationsdaten (E-Mail, Telefon, Nachrichteninhalte)	Kontaktaufnahme, Support, Beratung, Betrieb der E-Mail-Postfächer	Ansprechpartner, Absender und Empfänger von Nachrichten
Inhaltsdaten der Website (Texte, Bilder, Formulareingaben)	Erstellung, Pflege und Betrieb der Website	Kunden des Auftraggebers, Besucher der Website
Nutzungsdaten (IP-Adresse, Zugriffszeitpunkt, Seitenaufrufe)	Betrieb, Sicherheit und Reichweitenmessung der Website	Besucher der Website
Vertrags- und Abrechnungsdaten	Vertragsabwicklung, Rechnungsstellung, Zahlungsabwicklung	Kunden des Auftraggebers

Die Verarbeitung erfolgt für die Dauer des Hauptvertrages. Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO sind nicht Gegenstand des Auftrags; der Auftraggeber übermittelt solche Daten nur nach vorheriger gesonderter Vereinbarung.

Anlage 2: Unterauftragnehmer

Unterauftragnehmer	Anschrift	Leistungsumfang	Ort der Verarbeitung
WebPros International GmbH (Sitejet, Plesk)	Vordergasse 59, 8200 Schaffhausen, Schweiz	Hosting, Website-System, E-Mail-Postfächer, Domainverwaltung	Schweiz — Angemessenheitsbeschluss
Google Ireland Limited	Gordon House, Barrow Street, Dublin 4, Irland	E-Mail und Dateiablage, Web-Analyse, Werbeanzeigen	EU; Drittland nach Standardvertragsklauseln
Anthropic Ireland, Limited	Dublin, Irland	KI-gestützte Bearbeitung von Kunden- und Projektdaten	EU; Drittland nach Standardvertragsklauseln
Haufe-Lexware GmbH & Co. KG	Munzinger Straße 9, 79111 Freiburg, Deutschland	Buchhaltungs- und Rechnungssoftware	Deutschland
PayPal (Europe) S.à r.l. et Cie, S.C.A.	22-24 Boulevard Royal, L-2449 Luxemburg	Zahlungsabwicklung	EU
GitHub, Inc.	88 Colin P. Kelly Jr. Street, San Francisco, CA 94107, USA	Versionierte Sicherung der eigenen Arbeitsunterlagen	USA; Drittland nach Standardvertragsklauseln

Anlage 3: Technische und organisatorische Maßnahmen

Der Auftragnehmer ist ein Einzelunternehmen ohne Beschäftigte. Die Verarbeitung erfolgt ausschließlich durch den Inhaber. Die nachstehenden Maßnahmen beschreiben den tatsächlichen Stand.

1. Vertraulichkeit

- Zugang zu den Arbeitsräumen haben nur der Inhaber und von ihm eingelassene Personen; die Räume sind nicht öffentlich zugänglich und werden bei Abwesenheit verschlossen.

Die Arbeitsrechner sind vollständig festplattenverschlüsselt und mit Bildschirmsperre gesichert. Sicherheitsupdates werden zeitnah eingespielt.

- Für jedes System besteht ein eigenes Benutzerkonto mit individuellem Passwort; Passwörter werden in einem Passwortspeicher verwaltet und nicht mehrfach verwendet. Zwei-Faktor-Authentifizierung wird genutzt, wo der Anbieter sie anbietet.
- Im Website-System bestehen rollenbasierte Berechtigungen; Kunden erhalten ausschließlich Zugriff auf ihr eigenes Projekt.
- Kundendaten werden nicht in Nebenkopien auf Wechseldatenträgern gehalten. Datenträger werden vor einer Weitergabe verschlüsselt gelöscht, Papierunterlagen mit Kundenbezug geschreddert.

- Agentur- und Verlagsdaten werden in getrennten Ablagen geführt.

2. Integrität

- Die Übertragung erfolgt verschlüsselt: Websites und Verwaltungsoberflächen über HTTPS, E-Mail-Postfächer über IMAP und SMTP mit SSL.
- Änderungen an Kundenprojekten werden im Website-System protokolliert und sind einem Benutzerkonto zuzuordnen.
- Der Arbeitsstand der eigenen Systemdateien wird versioniert geführt, sodass Änderungen nachvollziehbar und rückholbar sind.

3. Verfügbarkeit und Belastbarkeit

- Das Website-System des Hosters legt bei jeder Bearbeitung einer Website automatisch Sicherungsstände an (alle Unterseiten mit Layout, Inhalten und Gestaltung sowie die Sammlungen). Vorgehalten werden für 24 Stunden je ein Stand pro Stunde, für sieben Tage je ein Stand pro Tag und für 52 Wochen je ein Stand pro Woche, höchstens 400 Stände. Ohne Bearbeitung entsteht kein neuer Stand. Eine Rücksicherung löst der Auftragnehmer im Website-System aus.
- Für die E-Mail-Postfächer besteht beim Hoster keine laufende Sicherung. Endgültig gelöschte Nachrichten und Postfächer hält der Hoster nicht vor; Nachrichten, die aufbewahrt werden müssen, sichert der Auftraggeber selbst.
- Die eigenen Arbeitsunterlagen werden zusätzlich außerhalb des Arbeitsrechners versioniert gesichert (privates Repository bei GitHub, siehe Anlage 2).
- Für den Ausfall eines Systems bestehen dokumentierte Wiederanlaufschritte.

4. Überprüfung und Bewertung

- Die Liste der Unterauftragnehmer und die vergebenen Zugänge werden mindestens jährlich durchgesehen; nicht mehr benötigte Zugänge werden entzogen.
- Vor der Beauftragung eines neuen Dienstleisters wird geprüft, ob ein Auftragsverarbeitungsvertrag vorliegt und wo verarbeitet wird.
- Neue Systeme werden datenschutzfreundlich voreingestellt; es werden nur die Daten erhoben, die für den Zweck erforderlich sind (Art. 25 DSGVO).

Anlage 4: Ansprechpartner für den Datenschutz

Name	Kontakt
Daniel Hmaidan, Inhaber	Telefon 02771 26 89 857 · service@hmaidan.de