

Auftragsverarbeitungsvertrag (AVV)

Fassung Juni 2026 · gültig bis 2. 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. Vertragsgegenstand

1. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.
2. Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

2. Gegenstand des Auftrags

Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in Anlage 1 zu diesem Vertrag festgelegt.

3. Rechte und Pflichten des Auftraggebers

3.1 Verantwortlichkeit des Auftraggebers

1. Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht nach Ziff. 4 Abs. 5 das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.
2. Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen.
3. Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen können in Textform (z. B. E-Mail) erfolgen.
4. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.
5. Der Auftraggeber kann weisungsberechtigte Personen benennen. Änderungen sind dem Auftragnehmer in Textform mitzuteilen.
6. Der Auftraggeber informiert den Auftragnehmer unverzüglich über Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener

Daten durch den Auftragnehmer. 3.2 Informationspflichten

7. Falls eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

4. Allgemeine Pflichten des Auftragnehmers

4.1 Verarbeitung nach Weisung

1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen.
2. Der Auftragnehmer verpflichtet sich, die Datenverarbeitung nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen. 4.2 Datensicherheit und Schutzmaßnahmen
3. Der Auftragnehmer sichert die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu.
4. Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten im erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. Änderungen sind vorab mit dem Auftraggeber abzustimmen. 4.3 Weisungen und Haftung
5. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer kann die Durchführung aussetzen, bis eine Klärung erfolgt.
6. Die Verarbeitung von Daten außerhalb der Betriebsstätten des Auftragnehmers oder Subunternehmern ist nur mit schriftlicher Zustimmung des Auftraggebers zulässig.
7. Der Auftragnehmer verarbeitet die Daten getrennt von anderen Datenbeständen.

5. Datenschutzbeauftragter des Auftragnehmers

5.1 Bestellung und Kontaktdaten

1. Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat.
2. Die Kontaktdaten des Datenschutzbeauftragten sind in Anlage 4 aufgeführt.

6. Meldepflichten des Auftragnehmers

6.1 Meldung von Datenschutzverstößen

1. Der Auftragnehmer ist verpflichtet, den Auftraggeber unverzüglich über Verstöße gegen Datenschutzrecht oder vertragliche Vereinbarungen zu informieren.
2. Die Meldung muss insbesondere folgende Informationen enthalten: • Beschreibung der Art der Datenschutzverletzung, • Kategorien und ungefähre Zahl der betroffenen Personen, • Maßnahmen zur Behebung der Verletzung.

7. Unterauftragnehmer

1. Der Auftragnehmer darf Unterauftragnehmer nur mit Zustimmung des Auftraggebers beauftragen. Diese sind in Anlage 2 aufzuführen.
2. Der Auftragnehmer stellt sicher, dass die gleichen Datenschutzpflichten wie in diesem Vertrag auch für die Unterauftragnehmer gelten.

8. Dauer und Beendigung

1. Der Vertrag beginnt mit Unterzeichnung und gilt auf unbestimmte Zeit.
2. Er kann mit einer Frist von drei Monaten zum Quartalsende gekündigt werden.
3. Nach Vertragsende hat der Auftragnehmer sämtliche personenbezogenen Daten zurückzugeben oder zu löschen. Die Löschung ist zu dokumentieren.

9. Schlussbestimmungen

1. Änderungen dieses Vertrags bedürfen der Schriftform.
2. Sollte eine Bestimmung dieses Vertrags unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Anlage 1: Gegenstand des Auftrags

Kategorie personenbezogener Daten	Zweck der Verarbeitung	Betroffene Personen
Kundendaten (z. B. Name, Anschrift)	Identifikation und Erbringung der vereinbarten Dienstleistungen, einschließlich Anmeldungen	Kunden des Auftraggebers
Kommunikationsdaten (z. B. E-Mail, Telefon)	Kontaktaufnahme, Support und Beratung	Nutzer von Support- und Beratungsangeboten
IT-Daten (z. B. IP-Adresse)	Betrieb der Website, Analyse der Zugriffe zur Verbesserung der Dienste	Besucher der Website
Vertrags- und Abrechnungsdaten	Vertragsabwicklung, Rechnungsstellung, Zahlungsabwicklung	Kunden des Auftraggebers

Anlage 2: Unterauftragnehmer

Unterauftragnehmer	Anschrift	Leistungsumfang
WebPros International GmbH (Sitejet, Plesk)	Vordergasse 59, 8200 Schaffhausen, Schweiz	Hosting, Website-System, E-Mail-Postfächer, Domainverwaltung
Google Ireland Limited	Gordon House, Barrow Street, Dublin 4, Irland	Cloud-Dienste, Web-Analyse, Werbeanzeigen

Unterauftragnehmer	Anschrift	Leistungsumfang
Anthropic Ireland, Limited	Dublin, Irland	KI-gestützte Bearbeitung von Kunden- und Projektdaten
Haufe-Lexware GmbH & Co. KG	Munzinger Straße 9, 79111 Freiburg, Deutschland	Buchhaltungs- und Rechnungssoftware
PayPal (Europe) S.à r.l. et Cie, S.C.A.	22-24 Boulevard Royal, L-2449 Luxemburg	Zahlungsabwicklung
Stripe Payments Europe, Ltd.	The One Building, 1 Grand Canal Street Lower, Dublin 2, Irland	Zahlungsabwicklung

Anlage 3: Technische und organisatorische Maßnahmen (TOMs)

1. Vertraulichkeit

1.1 Zutrittskontrolle

- Zu- und Ausgänge des Gebäudes sind permanent verschlossen, von außen nicht zu öffnen.
- Besucher werden durch Mitarbeiter begleitet.

1.2 Zugangskontrolle:

- Zuordnung von Benutzerrechten.
- Erstellen von Benutzerprofilen.
- Authentifikation von Benutzern durch Benutzername und Passwort.
- Passwortregeln mit Mindestzeichenzahl und Komplexitätsanforderungen.
- Automatisierte Kontrolle der Passwortregeln.
- Vorläufig vergebene Passwörter werden bei erster Anmeldung durch sichere Individualpasswörter ersetzt.
- Freigabe nur durch Administrator.
- Anti-Viren-Software, Firewall und regelmäßige Updates.
- Trennung von Firmennetz und Gäste-WLAN.
- Mobile-Device-Management-Software für Passwortänderungen.

1.3 Zugriffskontrolle:

- Verwendung nur geprüfter und freigegebener mobiler Datenträger.
- Rollenbasierte Berechtigungen nach Kategorien und Rechten.
- Separate Administratorkonten.
- Sichere Vernichtung von Datenträgern durch Zerstörung.
- Sichere Vernichtung von Akten und Datenträgervernichtung.

1.4 Pseudonymisierung & Verschlüsselung:

- Pseudonymisierung durch Kundennummer möglich.

2. Integrität

- Protokollierung der Einrichtung und des Betriebs von IT-Systemen.
- Sicherheitsmaßnahmen zur Kontrolle der Datenintegrität.
- Einsatz von sicheren Authentifizierungsverfahren.
- Verpflichtung der Mitarbeiter auf das Datengeheimnis.

3. Verfügbarkeit und Belastbarkeit

- Backup-Konzepte und regelmäßige Datensicherung.
- Redundante Speichersysteme zur Sicherstellung der Verfügbarkeit.
- Notfallkonzepte für den Wiederherstellungsprozess.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Regelmäßige Schulung und Sensibilisierung der Mitarbeiter.
- Verpflichtung der Mitarbeiter zur Einhaltung der Datenschutzrichtlinien.
- Überprüfung von externen Dienstleistern auf Datenschutzkonformität.
- Verarbeitung nur gemäß Art. 25 DSGVO.

Anlage 4: Datenschutzbeauftragter

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