AVV

Vertrag zur Auftragsverarbeitung

nach Art. 28 DSGVO, für alle Kundinnen und Kunden von Kavoma

INHALT

01 § 1 Parteien und Vertragsschluss
02 § 2 Gegenstand und Dauer
03 § 3 Art und Zweck der Verarbeitung
04 § 4 Art der Daten und betroffene Personen
05 § 5 Weisungen
06 § 6 Pflichten des Auftragnehmers
07 § 7 Technische und organisatorische Maßnahmen
08 § 8 Unterauftragnehmer
09 § 9 Unterstützung des Auftraggebers
10 § 10 Meldung von Datenschutzverletzungen
11 § 11 Nachweise und Kontrollen
12 § 12 Rückgabe und Löschung
13 § 13 Haftung und Schlussbestimmungen
14 Anlage 1: Technische und organisatorische Maßnahmen
15 Anlage 2: Unterauftragnehmer

KUNDE	PROJEKT	DATUM	VERSION
Geschäftskunden	Auftragsverarbeitung	18.11.2026	1.0

§ 1 Parteien und Vertragsschluss

(1) Dieser Vertrag gilt zwischen dem Kunden als Verantwortlichem (nachfolgend „Auftraggeber“) und Kavoma, Inhaber Artjom Kaufmann, Wehinger Weg 10, 78583 Böttingen, als Auftragsverarbeiter (nachfolgend „Auftragnehmer“).

(2) Er wird Bestandteil jedes Vertrags, bei dem der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers verarbeitet. Er gilt mit dem Vertragsschluss nach den Allgemeinen Geschäftsbedingungen von Kavoma als vereinbart. Das elektronische Format genügt nach Art. 28 Abs. 9 DSGVO. Auf Wunsch unterzeichnen die Parteien ihn zusätzlich.

(3) Begriffe wie „personenbezogene Daten“, „Verarbeitung“ und „Verletzung des Schutzes personenbezogener Daten“ haben die Bedeutung aus Art. 4 der Datenschutz-Grundverordnung (DSGVO).

§ 2 Gegenstand und Dauer

(1) Gegenstand ist die Verarbeitung personenbezogener Daten bei der Erbringung der Leistungen, die der Auftraggeber bei Kavoma gebucht hat, etwa Hosting, Domains, E-Mail-Dienste, die Erstellung und Pflege von Websites und Software, IT-Support und IT-Sicherheit.

(2) Der Vertrag gilt, solange der Auftragnehmer personenbezogene Daten für den Auftraggeber verarbeitet. Er endet nicht vor Abschluss der Rückgabe und Löschung nach § 12.

(3) Bei Widersprüchen zu anderen Vereinbarungen gehen in Fragen des Datenschutzes die Regelungen dieses Vertrags vor, außer die Parteien haben einen eigenen Vertrag zur Auftragsverarbeitung geschlossen. Dann gilt dieser.

§ 3 Art und Zweck der Verarbeitung

Der Auftragnehmer verarbeitet personenbezogene Daten nur, soweit es für die gebuchten Leistungen nötig ist:

Leistung	Art der Verarbeitung
Hosting	Speichern und Bereitstellen von Websites und Anwendungen einschließlich Datenbanken, Formularen und hochgeladenen Dateien; technisch nötige Server-Protokolle mit IP-Adressen der Besucher
Datensicherung	automatische Sicherung im Umfang des gebuchten Pakets und Wiederherstellung im Bedarfsfall

Leistung	Art der Verarbeitung
Domains und DNS	Verwaltung von Domains und DNS-Einträgen
E-Mail und Microsoft 365	Einrichtung, Migration und Verwaltung von Postfächern und Benutzern als Administrator im Auftrag des Auftraggebers
Websites und Software	Entwicklung, Test, Pflege und Fehlerbehebung, soweit dabei Inhalte oder Datenbanken mit personenbezogenen Daten verarbeitet werden
IT-Support und Fernwartung	Einsicht in Systeme und Daten, soweit es im Einzelfall für eine Anfrage, Fehlersuche oder Wartung nötig ist
Überwachung	Prüfen der Erreichbarkeit und der Funktion von Systemen und Sicherungen

Der Auftragnehmer nutzt die Daten nicht für eigene Zwecke wie Werbung oder Auswertungen. Er gibt sie nicht an Dritte weiter, außer nach diesem Vertrag.

§ 4 Art der Daten und betroffene Personen

(1) Je nach Leistung können folgende Arten von Daten betroffen sein:

- Kontaktdaten wie Name, Anschrift, E-Mail-Adresse und Telefonnummer
- Vertrags-, Kunden- und Mitgliedsdaten des Auftraggebers
- Zahlungs- und Buchhaltungsdaten
- Inhalte von E-Mails, Anhängen, Kalendern, Kontakten und Dokumenten
- Eingaben in Formulare und Inhalte von Websites und Anwendungen
- technische Daten wie IP-Adressen, Zeitpunkte von Zugriffen und Gerätedaten
- Zugangsdaten zu Benutzerkonten

(2) Verarbeitet der Auftraggeber besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO, etwa Gesundheitsdaten, oder Daten über strafrechtliche Verurteilungen, teilt er dies dem Auftragnehmer vorher mit. Die Parteien stimmen dann ab, ob zusätzliche Schutzmaßnahmen nötig sind.

(3) Betroffen sein können insbesondere Kunden, Interessenten und Mitglieder des Auftraggebers, Besucher seiner Websites, seine Beschäftigten sowie Geschäftspartner und Dienstleister.

§ 5 Weisungen

(1) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers, auch in Bezug auf die Übermittlung in ein Drittland. Ausgenommen sind Verarbeitungen, zu denen ihn das Recht der EU oder eines Mitgliedstaats verpflichtet. Dann teilt er dem Auftraggeber diese Pflicht vorher mit, sofern das Recht dies nicht verbietet.

(2) Die Weisungen ergeben sich aus diesem Vertrag und den gebuchten Leistungen. Einzelweisungen erteilt der Auftraggeber in Textform, etwa per E-Mail oder über das Kundenportal. Mündliche Weisungen bestätigt er unverzüglich in Textform.

(3) Weisungsberechtigt sind die gesetzlichen Vertreter des Auftraggebers und die Personen, die er dem Auftragnehmer in Textform benennt. Weisungen nimmt beim Auftragnehmer Artjom Kaufmann entgegen.

(4) Hält der Auftragnehmer eine Weisung für rechtswidrig, informiert er den Auftraggeber unverzüglich. Er darf die Ausführung aussetzen, bis der Auftraggeber sie bestätigt oder ändert.

§ 6 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet die Daten grundsätzlich in der EU und im Europäischen Wirtschaftsraum. Eine Übermittlung in ein Drittland erfolgt nur, wenn die Voraussetzungen der Art. 44 bis 49 DSGVO erfüllt sind. Für die in Anlage 2 genannten Unterauftragnehmer gilt die Zustimmung des Auftraggebers als erteilt.

(2) Der Auftragnehmer setzt nur Personen ein, die auf Vertraulichkeit verpflichtet sind oder einer gesetzlichen Verschwiegenheitspflicht unterliegen. Derzeit verarbeitet ausschließlich der Inhaber die Daten. Weitere Mitarbeitende setzt der Auftragnehmer erst nach schriftlicher Verpflichtung auf Vertraulichkeit und Datenschutz ein und gibt ihnen nur die Zugriffe, die sie für ihre Aufgaben brauchen. Die Vertraulichkeit gilt auch nach Vertragsende.

(3) Der Auftragnehmer führt ein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO.

(4) Ein Datenschutzbeauftragter ist beim Auftragnehmer gesetzlich nicht vorgeschrieben und nicht bestellt. Ansprechpartner für Datenschutz ist Artjom Kaufmann, info@kavoma.com, Telefon +49 1575 2985185.

(5) Zugangsdaten des Auftraggebers verwendet der Auftragnehmer nur für die vereinbarten Leistungen und bewahrt sie verschlüsselt auf.

(6) Personenbezogene Daten aus den Systemen des Auftraggebers übermittelt der Auftragnehmer nicht an Dienste der künstlichen Intelligenz. KI-Funktionen für den Auftraggeber setzt er nur nach

gesonderter Vereinbarung ein. Die dafür eingesetzten Anbieter werden dann als Unterauftragnehmer nach § 8 aufgenommen.

§ 7 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer trifft die Maßnahmen nach Art. 32 DSGVO, die in Anlage 1 beschrieben sind. Sie gewährleisten ein dem Risiko angemessenes Schutzniveau unter Berücksichtigung des Stands der Technik, der Kosten, der Art der Verarbeitung und der Risiken für die betroffenen Personen.

(2) Der Auftragnehmer darf die Maßnahmen weiterentwickeln, solange das Schutzniveau nicht sinkt. Wesentliche Änderungen dokumentiert er und veröffentlicht die aktuelle Fassung dieses Vertrags auf kavoma.com/avv/.

§ 8 Unterauftragnehmer

(1) Der Auftraggeber erteilt die allgemeine Genehmigung, Unterauftragnehmer einzusetzen. Die derzeit eingesetzten Unterauftragnehmer sind in Anlage 2 aufgeführt und gelten als genehmigt.

(2) Will der Auftragnehmer einen Unterauftragnehmer hinzufügen oder ersetzen, informiert er den Auftraggeber mindestens 30 Tage vorher in Textform. Der Auftraggeber kann innerhalb von 14 Tagen nach der Information aus wichtigem datenschutzrechtlichem Grund widersprechen. Finden die Parteien keine Lösung, kann jede Partei die betroffene Leistung außerordentlich kündigen.

(3) Der Auftragnehmer verpflichtet jeden Unterauftragnehmer vertraglich auf Datenschutzpflichten, die denen dieses Vertrags entsprechen. Er bleibt gegenüber dem Auftraggeber für deren Einhaltung verantwortlich.

(4) Keine Unterauftragsverhältnisse sind Nebenleistungen ohne Zugriff auf Daten des Auftraggebers, etwa Telekommunikation, Post- und Transportdienste oder die Wartung von Hardware.

(5) Schließt der Auftraggeber selbst Verträge mit Anbietern wie Microsoft für Microsoft 365, sind diese Anbieter keine Unterauftragnehmer des Auftragnehmers. Dann gelten deren Datenschutzbedingungen unmittelbar zwischen dem Auftraggeber und dem Anbieter. Der Auftragnehmer handelt in solchen Umgebungen nur als vom Auftraggeber beauftragter Administrator nach diesem Vertrag.

(6) Vergabestellen und Registrare für Domains, etwa die DENIC eG, erhalten die Daten des Domaininhabers in eigener Verantwortung, soweit sie für die Registrierung nötig sind.

§ 9 Unterstützung des Auftraggebers

(1) Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten Maßnahmen dabei, Anträge betroffener Personen nach Art. 12 bis 23 DSGVO zu beantworten, etwa auf Auskunft, Berichtigung, Löschung oder Datenübertragung. Wendet sich eine betroffene Person direkt an den Auftragnehmer, leitet er die Anfrage unverzüglich an den Auftraggeber weiter.

(2) Er unterstützt den Auftraggeber außerdem bei der Sicherheit der Verarbeitung, bei Meldungen von Datenschutzverletzungen, bei einer Datenschutz-Folgenabschätzung und bei einer Konsultation der Aufsichtsbehörde nach Art. 32 bis 36 DSGVO.

(3) Den Aufwand für diese Unterstützung kann der Auftragnehmer nach seinen Allgemeinen Geschäftsbedingungen berechnen, soweit er nicht durch einen Verstoß des Auftragnehmers verursacht wurde.

§ 10 Meldung von Datenschutzverletzungen

(1) Der Auftragnehmer meldet dem Auftraggeber eine Verletzung des Schutzes personenbezogener Daten unverzüglich, möglichst innerhalb von 24 Stunden, nachdem sie ihm bekannt geworden ist. Er meldet sie telefonisch und zusätzlich in Textform.

(2) Die Meldung enthält, soweit bekannt, die Art der Verletzung, die Kategorien und die ungefähre Zahl der betroffenen Personen und Datensätze, die wahrscheinlichen Folgen sowie die ergriffenen und vorgeschlagenen Maßnahmen. Fehlende Angaben reicht er unverzüglich nach.

(3) Der Auftragnehmer trifft sofort die nötigen Maßnahmen, um die Daten zu schützen und Folgen zu mindern. Meldungen an die Aufsichtsbehörde und Benachrichtigungen betroffener Personen nach Art. 33 und 34 DSGVO bleiben Sache des Auftraggebers. Der Auftragnehmer unterstützt ihn dabei, die Frist von 72 Stunden einzuhalten.

§ 11 Nachweise und Kontrollen

(1) Der Auftragnehmer stellt dem Auftraggeber auf Anfrage alle Informationen zur Verfügung, die zum Nachweis der Pflichten aus Art. 28 DSGVO nötig sind.

(2) Der Auftraggeber oder ein von ihm beauftragter, zur Verschwiegenheit verpflichteter Prüfer darf die Einhaltung dieses Vertrags überprüfen, auch vor Ort. Prüfungen werden mindestens 14 Tage vorher angekündigt, finden zu üblichen Geschäftszeiten statt und dürfen den Betrieb nicht unverhältnismäßig stören. Ohne konkreten Anlass findet höchstens eine Prüfung im Jahr statt.

(3) Ein Prüfer darf nicht im Wettbewerb zum Auftragnehmer stehen. Die Rechte der Aufsichtsbehörden bleiben unberührt.

§ 12 Rückgabe und Löschung

(1) Nach Ende der Leistungen gibt der Auftragnehmer nach Wahl des Auftraggebers alle personenbezogenen Daten zurück oder löscht sie, soweit keine gesetzliche Pflicht zur Aufbewahrung besteht. Der Auftraggeber teilt seine Wahl innerhalb von 30 Tagen nach Vertragsende mit. Ohne Mitteilung löscht der Auftragnehmer die Daten nach Ablauf dieser Frist.

(2) Die Rückgabe erfolgt in einem gängigen, maschinenlesbaren Format.

(3) Datensicherungen werden nicht einzeln gelöscht. Sie werden nach Ablauf ihrer Aufbewahrungsdauer automatisch überschrieben.

(4) Der Auftragnehmer bestätigt die Löschung auf Anfrage in Textform.

§ 13 Haftung und Schlussbestimmungen

(1) Für die Haftung gilt Art. 82 DSGVO. Im Verhältnis zwischen den Parteien gelten im Übrigen die Haftungsregeln der Allgemeinen Geschäftsbedingungen von Kavoma, soweit Art. 82 DSGVO nicht entgegensteht.

(2) Änderungen und Ergänzungen bedürfen der Textform. Änderungen dieses Vertrags kündigt der Auftragnehmer mindestens sechs Wochen vorher an. Für die Zustimmung gilt § 15 der Allgemeinen Geschäftsbedingungen entsprechend.

(3) Sollte eine Bestimmung unwirksam sein oder werden, bleiben die übrigen wirksam. An ihre Stelle tritt eine Regelung, die den Anforderungen des Art. 28 DSGVO entspricht.

(4) Es gilt das Recht der Bundesrepublik Deutschland.

Anlage 1: Technische und organisatorische Maßnahmen

Beschrieben sind die Maßnahmen des Auftragnehmers nach Art. 32 DSGVO. Die Maßnahmen der Unterauftragnehmer für Rechenzentren und Netze sind in deren eigenen Unterlagen beschrieben.

Vertraulichkeit

Bereich	Maßnahmen
Zutritt	Server stehen ausschließlich in Rechenzentren der Unterauftragnehmer mit Zutrittskontrolle. Der Auftragnehmer arbeitet in einem abschließbaren Büroraum, in dem keine Server stehen.
Zugang zu Systemen	Anmeldung an Servern nur per SSH-Schlüssel; Anmeldung mit Passwort und direkte Anmeldung als Administrator abgeschaltet; automatische Sperre nach wiederholten Fehlversuchen; Zwei-Faktor-Anmeldung für alle Verwaltungskonten bei Hosting-, Netz-, Cloud- und E-Mail-Anbietern; Verwaltungsoberflächen nur über eine zusätzliche Zugangsprüfung oder gar nicht aus dem Internet erreichbar
Netzwerk	Firewall beim Rechenzentrum, die nur benötigte Ports freigibt; Websites werden über einen Schutzdienst ausgeliefert, direkte Zugriffe auf die Server werden abgewiesen
Zugriff auf Daten	Zugriff nur durch den Inhaber oder verpflichtete Mitarbeitende im nötigen Umfang; Zugangsdaten verschlüsselt in einem Passwortmanager; Anwendungen verschiedener Kunden in getrennten Containern und Datenbanken
Arbeitsgeräte	Daten von Kunden nur auf verschlüsselten Datenträgern; automatische Bildschirmsperre; aktuelle Updates und Virenschutz; keine Speicherung auf privaten Geräten oder ungeschützten Wechseldatenträgern
Verschlüsselung	Übertragung ausschließlich verschlüsselt (HTTPS mit TLS, SSH); Datensicherungen werden verschlüsselt übertragen
Fernwartung	nur auf Anfrage oder mit Zustimmung des Auftraggebers für die einzelne Sitzung; verschlüsselte Verbindung

Integrität

Bereich	Maßnahmen
Weitergabe	Übertragung nur verschlüsselt; keine Weitergabe auf Datenträgern; Weitergabe nur an genehmigte Unterauftragnehmer
Eingabe und Änderungen	Protokollierung von Anmeldungen und administrativen Zugriffen auf den Servern; Änderungen an Websites und Einstellungen nachvollziehbar über Versionsverwaltung und Ticket-Verlauf

Bereich	Maßnahmen
Systemintegrität	automatische Sicherheitsupdates des Betriebssystems; regelmäßige Aktualisierung der eingesetzten Software; gehärtete Server-Konfiguration, geprüft mit anerkannten Prüfwerkzeugen

Verfügbarkeit und Belastbarkeit

Bereich	Maßnahmen
Datensicherung	automatische Sicherung der gehosteten Websites und Datenbanken im Umfang des gebuchten Pakets; kurzfristige Sicherungen auf dem Server, längerfristige auf einem getrennten Speicher in der EU
Wiederherstellung	dokumentierter Ablauf zur Wiederherstellung; regelmäßige Tests, ob sich Sicherungen zurückspielen lassen
Schutz vor Ausfällen	Schutz vor Überlastungsangriffen; Überwachung der Erreichbarkeit rund um die Uhr mit Benachrichtigung; Rechenzentrum mit redundanter Strom- und Netzversorgung

Überprüfung und Datenschutz

Bereich	Maßnahmen
Regelmäßige Prüfung	Überprüfung der Maßnahmen mindestens einmal im Jahr und nach Sicherheitsvorfällen
Datensparsamkeit	Verarbeitung nur der Daten, die für die Leistung nötig sind; Server-Protokolle mit IP-Adressen werden nur so lange gespeichert, wie es für Betrieb und Sicherheit nötig ist
Auftragskontrolle	Verarbeitung nur auf dokumentierte Weisung; Verträge zur Auftragsverarbeitung mit allen Unterauftragnehmern
Vorfälle	festgelegter Ablauf für Sicherheitsvorfälle mit Meldung an den Auftraggeber nach § 10

Anlage 2: Unterauftragnehmer

Unterauftragnehmer	Leistung	Ort der Verarbeitung	Garantien
netcup GmbH Daimlerstraße 25 76185 Karlsruhe	Server im Rechenzentrum, Registrierung von Domains	Nürnberg, Deutschland	Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO
Cloudflare, Inc. 101 Townsend St. San Francisco, CA 94107, USA	DNS, Schutz vor Angriffen und Weiterleitung des Datenverkehrs, Zugangsschutz, Speicher für Datensicherungen (Speicherort EU), Registrierung von Domains	Datensicherungen in der EU; Weiterleitung des Datenverkehrs über weltweite Rechenzentren, auch in den USA	Data Processing Addendum; EU-US Data Privacy Framework; EU-Standardvertragsklauseln
Microsoft Ireland Operations Limited One Microsoft Place, South County Business Park Leopardstown, Dublin 18, Irland	E-Mail und Dateiaustausch des Auftragnehmers, Anmeldung am Kundenportal für Mitarbeitende	EU, Zugriff aus den USA nicht ausgeschlossen	Vertrag zur Auftragsverarbeitung; EU-US Data Privacy Framework; EU-Standardvertragsklauseln
Capo System GmbH, Berlin	technische Betreuung der Microsoft-365-Umgebung und der Fernwartungs-Lizenz des Auftragnehmers	Deutschland	Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO
TeamViewer Germany GmbH Bahnhofsplatz 2 73033 Göppingen	Fernwartung	EU	Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO

Unterauftragnehmer	Leistung	Ort der Verarbeitung	Garantien
GitHub, Inc. 88 Colin P. Kelly Jr. St. San Francisco, CA 94107, USA	Ablage und Versionsverwaltung von Programmcode und Inhalten von Websites	USA	Data Protection Agreement; EU-US Data Privacy Framework; EU-Standardvertragsklauseln