

Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO

Stand: Sep 30, 2026

Vertragsparteien

zwischen

amr webdesign, Inhaber Reinhold Packeisen An der Landstraße 8, 26736 Krummhörn –
nachfolgend „Auftragnehmer“ –

und

Name / Firma: CSM Cologne Service Management GmbH Straße, Hausnummer:

Welser Str.10 g PLZ, Ort: 51149 Koeln

Kundennummer: 5123 – nachfolgend „Auftraggeber“ –

Präambel

Der Auftragnehmer erbringt für den Auftraggeber Webhosting- und E-Mail-Dienstleistungen auf Grundlage des zwischen den Parteien bestehenden Hauptvertrags (Auftragsbestätigung, Rechnungen und AGB unter der oben genannten Kundennummer). Die Leistungen werden auf Servern und virtuellen Servern erbracht, die der Auftragnehmer bei der Host Europe GmbH in deren Rechenzentrum in Deutschland betreibt und selbst verwaltet.

Dieser Vertrag konkretisiert die datenschutzrechtlichen Pflichten der Parteien gemäß Art. 28 DSGVO. Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag gehen die Regelungen dieses Vertrags vor.

§ 1 Gegenstand des Auftrags

1.1 Gegenstand ist die Bereitstellung von Webhosting, E-Mail-Postfächern, Datenbanken, Domainverwaltung sowie die technische Administration und Wartung der zugehörigen Server durch den Auftragnehmer.

1.2 Der Auftragnehmer verarbeitet personenbezogene Daten nicht zu eigenen Zwecken. Bei Speicherung, Datensicherung, Wartung, Fehlerbehebung und Support kann ein Zugriff auf personenbezogene Daten des Auftraggebers jedoch nicht ausgeschlossen werden. Insoweit handelt der Auftragnehmer als Auftragsverarbeiter.

1.3 Personenbezogene Daten im Sinne dieses Vertrags sind ausschließlich solche im Sinne von Art. 4 Nr. 1 DSGVO.

§ 2 Laufzeit

Dieser Vertrag gilt für die Dauer des Hauptvertrags über Hosting- und E-Mail-Leistungen. Er endet automatisch, wenn der Auftraggeber keine solchen Leistungen mehr bezieht. Pflichten nach § 11 (Löschung und Rückgabe) gelten darüber hinaus fort.

§ 3 Art, Zweck und Ort der Verarbeitung

3.1 Art der Verarbeitung: Speichern, Übermitteln (Ausliefern von Webseiten und E-Mails), Sichern, Wiederherstellen und Löschen von Daten.

3.2 Zweck: Betrieb der Websites und E-Mail-Dienste des Auftraggebers.

3.3 Die Server des Auftragnehmers stehen ausschließlich in Rechenzentren in der Bundesrepublik Deutschland. Eine Verlagerung in einen anderen Staat der EU oder des EWR bedarf der vorherigen Information des Auftraggebers; eine Verlagerung in ein Drittland bedarf seiner vorherigen schriftlichen Zustimmung und ist nur unter den Voraussetzungen der Art. 44 ff. DSGVO zulässig.

§ 4 Art der Daten und Kreis der Betroffenen

4.1 Art der Daten:

- Inhalte der Websites des Auftraggebers, einschließlich Datenbankinhalten (z. B. Nutzerkonten, Bestellungen, Buchungen)
- Formulardaten (z. B. Kontakt- und Anfrageformulare)
- E-Mail-Inhalte, Anhänge und Metadaten (Absender, Empfänger, Zeitstempel) sowie Postfachinhalte
- Server-Protokolldaten (IP-Adressen, Zugriffszeitpunkte, aufgerufene Seiten, Browserinformationen)
- Zugangsdaten zu Postfächern, FTP- und CMS-Konten
- Sonstige vom Auftraggeber gespeicherte Daten: _____

4.2 Kreis der Betroffenen:

- Besucher der Websites des Auftraggebers
- Kunden, Interessenten und Ansprechpartner des Auftraggebers
- Beschäftigte des Auftraggebers (insbesondere Postfachnutzer)
- E-Mail-Kommunikationspartner des Auftraggebers

- Sonstige: _____

4.3 Die Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO) ist nicht Gegenstand des Hostings. Beabsichtigt der Auftraggeber, solche Daten zu speichern, teilt er dies dem Auftragnehmer vorab mit.

§ 5 Weisungsgebundenheit

5.1 Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierter Weisung des Auftraggebers, auch in Bezug auf Übermittlungen in Drittländer (Art. 28 Abs. 3 lit. a DSGVO). Dies gilt nicht, soweit der Auftragnehmer durch Unionsrecht oder deutsches Recht zu einer Verarbeitung verpflichtet ist; in diesem Fall teilt er dem Auftraggeber diese Verpflichtung vorher mit, sofern das Recht dies nicht verbietet.

5.2 Weisungen erfolgen in Textform (z. B. per E-Mail). Mündliche Weisungen bestätigt der Auftraggeber unverzüglich in Textform.

5.3 Ist der Auftragnehmer der Ansicht, dass eine Weisung gegen Datenschutzvorschriften verstößt, weist er den Auftraggeber unverzüglich darauf hin (Art. 28 Abs. 3 S. 3 DSGVO). Er darf die Ausführung der Weisung aussetzen, bis der Auftraggeber sie bestätigt oder ändert.

5.4 Der Auftraggeber hat über die ihm bereitgestellten Zugänge (z. B. Plesk, CMS, Webmail, FTP) selbst umfassenden Zugriff auf seine Daten und kann Berichtigungen und Löschungen grundsätzlich eigenständig vornehmen.

§ 6 Pflichten des Auftragnehmers

6.1 Der Auftragnehmer verwendet die Daten nicht für andere Zwecke, insbesondere nicht für eigene Werbe- oder Marketingzwecke, und gibt sie nur an Dritte weiter, wenn dies nach § 7 zulässig oder gesetzlich vorgeschrieben ist. Kopien werden nur erstellt, soweit sie für den Betrieb, die Datensicherung oder zur Erfüllung gesetzlicher Pflichten erforderlich sind.

6.2 Der Auftragnehmer stellt sicher, dass alle Personen, die Zugriff auf die Daten haben können, zur Vertraulichkeit verpflichtet sind oder einer gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Bei E-Mail-Diensten wahrt er das Fernmeldegeheimnis nach § 3 TDDDG.

6.3 Der Auftragnehmer trifft die in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO. Er darf diese an den Stand der Technik anpassen, sofern das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen werden dokumentiert und dem Auftraggeber auf Anfrage mitgeteilt.

6.4 Der Auftragnehmer ist nicht zur Benennung eines Datenschutzbeauftragten verpflichtet. Ansprechpartner für Datenschutzfragen ist Reinhold Packeisen, E-Mail: buero@amrwebdesign.de, Telefon: +49 170 9080874.

§ 7 Unterauftragsverhältnisse

7.1 Der Auftraggeber erteilt eine allgemeine Genehmigung zur Beauftragung weiterer Auftragsverarbeiter (Art. 28 Abs. 2 DSGVO). Die bei Vertragsschluss eingesetzten Unterauftragnehmer sind in Anlage 1 aufgeführt und gelten als genehmigt. Die von der Host Europe GmbH ihrerseits eingesetzten Subunternehmer ergeben sich aus deren Subunternehmerliste, die der Auftragnehmer auf Anfrage zur Verfügung stellt. Über Änderungen dieser Liste, die dem Auftragnehmer mitgeteilt werden, informiert er den Auftraggeber unverzüglich.

7.2 Der Auftragnehmer informiert den Auftraggeber mindestens 4 Wochen vorab in Textform über jede beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragnehmers. Der Auftraggeber kann innerhalb von 2 Wochen nach Zugang aus wichtigem datenschutzrechtlichem Grund widersprechen. Kommt keine Einigung zustande, kann jede Partei die betroffene Leistung außerordentlich kündigen.

7.3 Der Auftragnehmer verpflichtet jeden Unterauftragnehmer vertraglich auf dieselben Datenschutzpflichten wie in diesem Vertrag (Art. 28 Abs. 4 DSGVO). Er haftet gegenüber dem Auftraggeber für die Einhaltung dieser Pflichten durch den Unterauftragnehmer.

7.4 Keine Unterauftragsverhältnisse sind Nebenleistungen wie Telekommunikations-, Post- und Transportdienste sowie die Wartung von Hardware ohne Zugriff auf personenbezogene Daten.

§ 8 Unterstützung bei Betroffenenrechten

8.1 Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner technischen Möglichkeiten bei der Erfüllung der Rechte Betroffener nach Kapitel III DSGVO, insbesondere Auskunft, Berichtigung, Löschung und Einschränkung (Art. 28 Abs. 3 lit. e DSGVO).

8.2 Wendet sich ein Betroffener direkt an den Auftragnehmer, leitet dieser die Anfrage unverzüglich an den Auftraggeber weiter und beantwortet sie nicht selbst.

8.3 Für Unterstützungsleistungen, die der Auftraggeber über seine eigenen Zugänge selbst erledigen könnte, kann der Auftragnehmer den nachgewiesenen Aufwand nach seinen üblichen Stundensätzen berechnen.

§ 9 Meldung von Datenschutzverletzungen

9.1 Der Auftragnehmer meldet dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnis, in Textform (Art. 33 Abs. 2 DSGVO).

9.2 Die Meldung enthält, soweit bekannt: Art der Verletzung, betroffene Datenkategorien und ungefähre Zahl der Betroffenen, wahrscheinliche Folgen sowie ergriffene oder vorgeschlagene Gegenmaßnahmen. Fehlende Angaben werden nachgereicht.

9.3 Der Auftragnehmer unterstützt den Auftraggeber bei dessen Pflichten nach Art. 32 bis 36 DSGVO (Meldung an die Aufsichtsbehörde, Benachrichtigung Betroffener, Datenschutz-Folgenabschätzung) im Rahmen der von ihm erbrachten Leistungen.

§ 10 Kontrollrechte des Auftraggebers

10.1 Der Auftragnehmer stellt dem Auftraggeber auf Anfrage alle Informationen zur Verfügung, die zum Nachweis der Einhaltung dieses Vertrags erforderlich sind (Art. 28 Abs. 3 lit. h DSGVO). Als Nachweis dienen insbesondere Anlage 2 sowie die Zertifizierungen des Rechenzentrumsbetreibers.

10.2 Der Auftraggeber oder ein von ihm beauftragter, zur Verschwiegenheit verpflichteter Prüfer kann nach Anmeldung mit einer Frist von 3 Wochen während der üblichen Geschäftszeiten und ohne Störung des Betriebs Kontrollen beim Auftragnehmer durchführen. Kontrollen beim Rechenzentrumsbetreiber richten sich nach dessen Bedingungen.

10.3 Den nachgewiesenen Aufwand für Vor-Ort-Kontrollen trägt der Auftraggeber, es sei denn, die Kontrolle deckt einen Verstoß des Auftragnehmers auf.

§ 11 Löschung und Rückgabe nach Vertragsende

11.1 Der Auftraggeber ist dafür verantwortlich, seine Daten (z. B. Website-Dateien, Datenbanken, E-Mails) vor dem Wirksamwerden der Kündigung selbst zu sichern, etwa über die Export- und Backup-Funktionen in Plesk. Auf Wunsch unterstützt der Auftragnehmer dabei gegen Berechnung des Aufwands.

11.2 Zum Zeitpunkt der Vertragsbeendigung löscht der Auftragnehmer sämtliche Daten des Auftraggebers auf den Servern (Webpace, Datenbanken, Postfächer, vom Auftraggeber in Plesk angelegte Backups). In den täglichen Serversicherungen des Auftragnehmers enthaltene Daten werden im regulären Sicherungszyklus überschrieben, spätestens nach 7 Tagen. Eine Wiederherstellung nach Vertragsende ist nicht geschuldet.

11.3 Dies gilt nicht, soweit gesetzliche Aufbewahrungspflichten bestehen. Nachweise über die ordnungsgemäße Auftragsverarbeitung (z. B. dieser Vertrag) darf der Auftragnehmer entsprechend den gesetzlichen Fristen aufbewahren.

11.4 Der Auftragnehmer bestätigt die Löschung auf Anfrage in Textform.

§ 12 Pflichten des Auftraggebers

12.1 Der Auftraggeber ist Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO und für die Rechtmäßigkeit der Verarbeitung, die Wahrung der Betroffenenrechte sowie seine Informationspflichten nach Art. 13 und 14 DSGVO (z. B. Datenschutzerklärung der Website) allein verantwortlich.

12.2 Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Verstöße gegen Datenschutzbestimmungen feststellt.

12.3 Der Auftraggeber ist für die Sicherheit der von ihm installierten Software (z. B. CMS, Plugins, Erweiterungen) und die Vertraulichkeit seiner Zugangsdaten verantwortlich, soweit deren Pflege nicht ausdrücklich im Hauptvertrag dem Auftragnehmer übertragen ist.

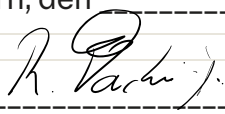
§ 13 Schlussbestimmungen

13.1 Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform. Der Vertrag kann auch in elektronischer Form geschlossen werden (Art. 28 Abs. 9 DSGVO).

13.2 Sollte eine Bestimmung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien ersetzen die unwirksame Bestimmung durch eine wirksame, die dem wirtschaftlichen Zweck am nächsten kommt. Gleiches gilt für Regelungslücken.

13.3 Es gilt deutsches Recht. Ist der Auftraggeber Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen, ist Gerichtsstand Emden.

Unterschriften

Auftraggeber	Auftragnehmer
Ort, Datum: _____	Krummhörn, den 30.9.2026
_____	 _____

Auftraggeber	Auftragnehmer
Name, Unterschrift	amr webdesign, Reinhold Packeisen

Anlage 1 – Unterauftragnehmer

Bei Vertragsschluss sind folgende Unterauftragnehmer genehmigt:

Unternehmen	Anschrift	Leistung	Ort der Verarbeitung
Host Europe GmbH	c/o WeWork, Friesenplatz 4, 50672 Köln	Bereitstellung und Betrieb der Server und VServer im Rechenzentrum, Netzanbindung, Speicherung der Serverbackups	Deutschland
Nethosting24 GmbH	Düsseldorfer Str. 81a, 40667 Meerbusch	Registrierung und Verwaltung von Domains (Domainrobot), Übermittlung der Domaininhaberdaten an die Registries	Deutschland

Der Spamfilter (SpamAssassin) läuft auf den Servern des Auftragnehmers und ist kein Unterauftragnehmer.

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

Die folgenden Maßnahmen beschreiben den Stand zum Vertragsdatum. Mit [prüfen] markierte Punkte bitte an die tatsächliche Umsetzung anpassen oder streichen.

1. Vertraulichkeit

Zutrittskontrolle (Rechenzentrum)

- Server stehen ausschließlich im Rechenzentrum der Host Europe GmbH in Deutschland
- Physische Sicherheit durch den Rechenzentrumsbetreiber: Zutrittskontrollsystem, Videoüberwachung, Sicherheitspersonal; Host Europe GmbH ist nach ISO/IEC 27001 zertifiziert
- Der Auftragnehmer selbst hat keinen physischen Zutritt zu den Servern

Zugangskontrolle (Systeme)

- Administration ausschließlich über verschlüsselte Verbindungen (HTTPS, SSH)
- SSH-Anmeldung nur per Schlüssel, Passwort-Login für root deaktiviert
- Zwei-Faktor-Authentifizierung für Plesk-Zugänge verfügbar; Nutzung durch den Auftraggeber optional und empfohlen
- Firewall auf allen Servern, nur benötigte Ports geöffnet
- Automatische Sperrung nach wiederholten Fehlanmeldungen (Fail2ban)
- Passwortrichtlinie: Mindestlänge 12 Zeichen, keine Mehrfachverwendung

Zugriffskontrolle

- Jeder Auftraggeber erhält eigene, voneinander getrennte Abonnements bzw. Benutzerkonten in Plesk
- Administrative Rechte liegen ausschließlich beim Auftragnehmer
- Zugriff auf Kundendaten durch den Auftragnehmer nur, soweit für Betrieb, Support oder Fehlerbehebung erforderlich

Trennungskontrolle

- Getrennte Webspaces, Datenbanken und Postfächer je Auftraggeber
- Getrennte Systembenutzer je Abonnement

2. Integrität

Weitergabekontrolle

- TLS-Verschlüsselung für Websites (HTTPS) mit automatisch erneuerten Zertifikaten
- Verschlüsselte Übertragung für E-Mail-Abruf und -Versand (IMAPS, POP3S, SMTP mit STARTTLS bzw. SMTPS)
- Dateiübertragung ausschließlich über SFTP (unverschlüsseltes FTP deaktiviert)

Eingabekontrolle

- Protokollierung von Anmeldungen und administrativen Vorgängen auf Systemebene
- Server-Logfiles werden nach 30 Tagen gelöscht

3. Verfügbarkeit und Belastbarkeit

- Redundante Stromversorgung, Klimatisierung und Brandschutz im Rechenzentrum (durch Host Europe)
- Tägliche Sicherung der Server durch den Auftragnehmer, Aufbewahrung 7 Tage (rollierend). Zusätzlich kann der Auftraggeber in Plesk eigene Backups seines Abonnements einrichten; für deren Einstellung, Umfang und Speicherort ist er selbst

verantwortlich. Die Aufbewahrung dieser Kundenbackups ist auf maximal einen Monat begrenzt

- Speicherort der Serverbackups: Backup-Speicher der Host Europe GmbH in Deutschland, getrennt vom Produktivsystem
- Wiederherstellung aus den Backups getestet und regelmäßig überprüft
- Spamfilter für eingehende E-Mails (SpamAssassin)
- Überwachung der Server-Verfügbarkeit über das Kundenpanel der Host Europe GmbH

4. Verfahren zur regelmäßigen Überprüfung

- Zeitnahes Einspielen von Sicherheitsupdates für Betriebssystem, Plesk und Serverdienste
- Regelmäßige Aktualisierung der vom Auftragnehmer betreuten CMS-Installationen, soweit im Hauptvertrag vereinbart
- Überprüfung dieser Maßnahmen mindestens einmal jährlich
- Schriftliche Verpflichtung aller Mitarbeiter und Hilfspersonen auf Vertraulichkeit