

Auftragsverarbeitung für Agenturleistungen

AVV 2.0 · Prüffassung vom 21.09.2026 · mit Anlagen C und E

Entwurf – noch nicht zum Abschluss freigegeben. Die Agentur ergänzt vor Verwendung das kundenspezifische Blatt (Anlagen A, B und D), bestätigt die tatsächlichen Sicherheitsmaßnahmen und schließt alle offenen Punkte. Fundierte Arbeitshilfe, kein Ersatz für anwaltliche Rechtsberatung.

1. Parteien, Gegenstand und Laufzeit

Auftragsverarbeiter ist Ing. Michael Kristen, handelnd als amWeb.digital.agency, Einzelunternehmen, Rieslinggasse 72, 2353 Guntramsdorf, Österreich (Agentur). Verantwortlicher ist der im Kundenblatt bezeichnete Rechtsträger (Kunde). Dieses Muster setzt voraus, dass der Kunde selbst Verantwortlicher ist. Für Kunden, die selbst Auftragsverarbeiter sind, muss die Weisungs- und Genehmigungskette gesondert angepasst werden.

Gegenstand, Art, Zweck, Dauer, Datenarten, betroffene Personen, Systeme, Verarbeitungsorte und Löschfristen werden im Kundenblatt festgelegt. Dieses enthält Anlagen A (Verarbeitung), B (Daten und Betroffene) und D (Unterauftragsverarbeiter). Anlagen C und E in diesem Dokument sowie die bestätigten Konkretisierungen im Kundenblatt sind verbindliche Vertragsbestandteile. Ein bloßer Verweis auf eine veränderbare Website ersetzt diese Festlegungen nicht.

Der AVV gilt mit nachweisbarem Abschluss durch beide Parteien für die bezeichneten Leistungen und bis zur vollständigen Rückgabe oder Löschung der Auftragsdaten. Er muss vor Beginn der Auftragsverarbeitung abgeschlossen sein. Eine spätere Vereinbarung wirkt nicht rückwirkend und beseitigt keine frühere Vertragslücke. Hauptvertrag und AVV werden im Abschlussblatt eindeutig bezeichnet.

2. Rollen und Weisungen

Der Kunde bestimmt die Zwecke und wesentlichen Mittel der Verarbeitung und verantwortet deren Rechtsgrundlagen, Informationspflichten und erforderliche Einwilligungen. Die Agentur entscheidet über die technische Umsetzung innerhalb der Weisungen. Ihre eigenen gesetzlichen Pflichten bleiben bestehen. Die Vereinbarung und das ausgefüllte Kundenblatt bilden die erste dokumentierte Weisung.

Weitere Weisungen, auch zu Drittlandübermittlungen, erfolgen durch die benannten Berechtigten per E-Mail oder über einen ausdrücklich vereinbarten dokumentierbaren Kanal. Mündliche Eilweisungen werden unverzüglich dokumentiert und vom Kunden bestätigt. Bei Zweifeln prüft die Agentur die Berechtigung. Hält sie eine Weisung für rechtswidrig, informiert sie den Kunden unverzüglich und setzt die betroffene Handlung bis zur rechtmäßigen Klärung aus.

Die Agentur verarbeitet Auftragsdaten ausschließlich auf dokumentierte Weisung. Verpflichtet sie Unionsrecht oder das Recht eines Mitgliedstaats ausnahmsweise zu einer anderen Verarbeitung, informiert sie den Kunden vorher über diese Anforderung, soweit das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet.

Die Agentur verwendet Auftragsdaten nicht für eigene Werbung, Profilbildung oder Modelltraining. Eigene Vertragsverwaltung und Rechnungslegung betreffen nur die dafür erforderlichen Geschäftsbeziehungsdaten und sind vom Auftrag getrennt. Eine Website-Abnahme allein ersetzt diesen AVV nicht. Ein allgemeiner Agenturauftrag erlaubt keine Übermittlung personenbezogener Daten an beliebige Cloud- oder KI-Dienste.

3. Vertraulichkeit und Sicherheit

Die Agentur setzt nur berechnigte, angemessen unterwiesene Personen ein, die zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeit besteht nach Tätigkeitsende fort. Zugriffe werden auf den notwendigen Umfang begrenzt und bei Wegfall des Bedarfs entzogen.

Die Agentur trifft die nach Art. 32 DSGVO erforderlichen Maßnahmen. Anlage C und ihre ausgefüllte Konkretisierung im Kundenblatt beschreiben die vereinbarten Maßnahmen. Auch bei ausgelagertem Hosting bleiben die Agenturmaßnahmen für Endgeräte, Zugänge, Anwendungen und Arbeitsabläufe

erforderlich. Die Agentur prüft die Wirksamkeit regelmäßig und anlassbezogen entsprechend dem Risiko und dokumentiert Ergebnisse und Abhilfe.

Technische Weiterentwicklungen sind zulässig, wenn das erforderliche und vereinbarte Schutzniveau erhalten bleibt. Wesentliche Änderungen werden dokumentiert und vorab mitgeteilt; dringende Schutzmaßnahmen werden unverzüglich nachträglich erläutert. Eine Absenkung des vereinbarten Schutzniveaus erfordert eine vorherige Vereinbarung und darf gesetzliche Mindestanforderungen nicht unterschreiten.

4. Unterstützung und Datenschutzverletzungen

Die Agentur unterstützt den Kunden angesichts der Verarbeitungsart nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von Betroffenenrechten nach Kapitel III DSGVO. Anträge leitet sie unverzüglich an den Kunden weiter; eine inhaltliche Antwort erfolgt nur auf Weisung oder aufgrund eigener gesetzlicher Pflicht.

Unter Berücksichtigung der Art der Verarbeitung und der verfügbaren Informationen unterstützt sie den Kunden bei Art. 32 bis 36 DSGVO, insbesondere bei Sicherheit, Datenschutzverletzungen, Datenschutz-Folgenabschätzung und vorheriger Konsultation. Sie beschafft erforderliche Informationen aus der Unterauftragskette.

Eine bekannt gewordene Verletzung des Schutzes der Auftragsdaten meldet die Agentur dem Kunden unverzüglich an den vereinbarten Kontakt. Verfügbare Angaben zu Art und Zeitpunkt, betroffenen Daten und Personen, ungefähren Anzahlen, Folgen, Abhilfe und Ansprechpartner werden mitgeteilt; fehlende Informationen werden ohne vermeidbare Verzögerung nachgereicht. Die Agentur sichert erforderliche Nachweise und dokumentiert Verlauf und Maßnahmen. Erhebliche Verdachtsfälle kennzeichnet und meldet sie als solche.

Der Kunde entscheidet über seine Behördenmeldungen und Benachrichtigungen Betroffener. Eigene gesetzliche Pflichten der Agentur bleiben unberührt. Die 72-Stunden-Frist des Art. 33 Abs. 1 DSGVO berechtigt die Agentur nicht zum Zuwarten. Zusätzliche feste Meldefristen gelten nur, wenn sie ausdrücklich und nach Prüfung ihrer Umsetzbarkeit vereinbart werden.

5. Unterauftragsverarbeitung und Drittlandübermittlungen

Mit Abschluss erteilt der Kunde eine allgemeine schriftliche Genehmigung zur Beauftragung weiterer Auftragsverarbeiter unter den Bedingungen dieses AVV. Der Ausgangsbestand wird ausschließlich durch die vollständig ausgefüllte und bestätigte Anlage D bestimmt. Geplante Ergänzungen und Ersetzungen, auch auf weiteren Stufen, unterliegen dem Informations- und Widerspruchsverfahren in Anlage E. Ungeklärte Prüfkandidaten sind keine genehmigten Anbieter.

Sofern das Kundenblatt Hosting über den Agentur-Account bei World4You vorsieht, wird World4You Internet Services GmbH ausdrücklich als Unterauftragsverarbeiter für Hosting, Speicherung, Datensicherung und technische Bereitstellung im dort festgelegten Paketumfang benannt. Bei einem Direktvertrag des Kunden mit seinem Hoster ist dieser Hoster nicht allein deshalb Unterauftragsverarbeiter der Agentur. Getrennte Dienste der Agentur, etwa ein eigener Analyse-Server, sind gesondert zuzuordnen.

Die Agentur prüft vor Einsatz ausreichende Garantien und verpflichtet weitere Auftragsverarbeiter durch Vertrag zu denselben Datenschutzpflichten, die ihr aus diesem AVV obliegen, insbesondere zu geeigneter Sicherheit und ausreichender Unterstützung. Entsprechende Pflichten und Transparenz müssen auch auf weiteren Stufen bestehen. Die Agentur bleibt gegenüber dem Kunden für die Erfüllung der Pflichten weiterer Auftragsverarbeiter nach Art. 28 Abs. 4 DSGVO verantwortlich.

Anlage D benennt die tatsächlich eingesetzten Rechtsträger, Leistungen, Daten, Orte einschließlich Fernzugriffen sowie weitere Stufen oder eine beigefügte, eindeutig versionierte vollständige Liste. Die Agentur hält diese Angaben aktuell und stellt die erforderlichen Nachweise zur Verfügung. Eine bloße Liste sämtlicher theoretisch möglicher Hersteller genügt nicht.

Verarbeitung oder Zugriff außerhalb des EWR erfolgt nur auf dokumentierte Weisung und bei erfüllten Voraussetzungen des Kapitels V DSGVO. Betroffene Staaten, Empfänger, Übermittlungsgrundlage und erforderliche ergänzende Maßnahmen werden vorab dokumentiert. Ein AVV allein legitimiert keine

Drittlandübermittlung. Neue Datenflüsse dürfen erst nach abgeschlossener Prüfung und erforderlicher vertraglicher Festlegung beginnen.

6. Nachweise und Kontrollen

Die Agentur stellt dem Kunden alle Informationen zur Verfügung, die zum Nachweis der Einhaltung dieses AVV und des Art. 28 DSGVO erforderlich sind. Sie ermöglicht Überprüfungen einschließlich Inspektionen durch den Kunden oder einen von ihm beauftragten Prüfer und wirkt daran mit. Die Rechte dürfen nicht ausschließlich auf einen vom Dienstleister selbst ausgewählten Prüfer beschränkt werden.

Kontrollen werden grundsätzlich rechtzeitig abgestimmt und verhältnismäßig durchgeführt. Geheimnisse und Daten anderer Kunden werden geschützt. Geeignete Berichte oder Zertifikate können einbezogen werden, ersetzen eine erforderliche Kontrolle aber nicht. Dringende Vorfälle oder behördliche Anforderungen ermöglichen entsprechend kurzfristige Kontrollen.

7. Rückgabe, Löschung und Aufbewahrung

Nach Abschluss der Leistungen gibt die Agentur nach Wahl des Kunden sämtliche Auftragsdaten zurück oder löscht sie und löscht vorhandene Kopien, soweit keine gesetzliche Pflicht nach Unionsrecht oder dem Recht eines Mitgliedstaats zur weiteren Speicherung besteht. Format, Übergabeweg, operative Löschfrist und maximaler Ablauf verbleibender Sicherungskopien stehen im Kundenblatt. Nachweise der Umsetzung werden auf Verlangen bereitgestellt.

Bis zum festgelegten Ablauf unveränderbarer Sicherungen werden diese vom regulären Betrieb getrennt, zugriffsbeschränkt und nur zu erforderlicher Wiederherstellung verwendet. Bei einer Wiederherstellung wird die Löschanweisung erneut umgesetzt. Eine unbegrenzte oder unbestimmte Backup-Aufbewahrung wird nicht vereinbart. Gesetzlich zwingend gespeicherte Daten werden auf das Erforderliche beschränkt; Grundlage und Dauer werden dem Kunden mitgeteilt, soweit zulässig.

Ein allgemeines Interesse der Agentur an Vertragsnachweisen rechtfertigt nicht die Aufbewahrung vollständiger Website-, Formular- oder Nutzerdaten. Erforderliche Vertrags- und Erfüllungsnachweise werden getrennt und datensparsam behandelt.

8. Kosten, Rangfolge und Änderungen

Die Vergütung richtet sich nach dem Hauptvertrag und ergänzenden Vereinbarungen. Gesetzlich notwendige Schutz- und Unterstützungshandlungen dürfen nicht wegen einer ungeklärten Vergütung oder Vorauszahlung verzögert werden. Aus eigenem Pflichtverstoß erforderliche Abhilfe wird nicht als Zusatzleistung berechnet.

Bei Widersprüchen über die Auftragsverarbeitung geht dieser AVV vor. Im Übrigen bleiben wirksam vereinbarte kaufmännische Bedingungen bestehen. Zwingende Rechte betroffener Personen sowie Pflichten und Haftung insbesondere aus Art. 28 Abs. 4 und Art. 82 DSGVO werden nicht eingeschränkt. Eine darüber hinausgehende pauschale verschuldensunabhängige Haftung wird mit diesem AVV nicht begründet.

Materielle Änderungen dieses Vertrags und Erweiterungen der Verarbeitung bedürfen einer nachweisbaren Vereinbarung, schriftlich auch in elektronischem Format im Sinne von Art. 28 Abs. 9 DSGVO. Das gesondert vereinbarte Verfahren für Unterauftragsverarbeiter und gleichwertige Sicherheitsfortentwicklungen bleibt anwendbar. Eine Veröffentlichung geänderter Texte auf der Website ersetzt keine erforderliche Vereinbarung oder Mitteilung.

Anlage C – Technische und organisatorische Maßnahmen

Verbindliches Maßnahmenmodell zur Konkretisierung vor Abschluss. Die folgenden Maßnahmen werden für den vereinbarten Umfang geschuldet. Die Agentur muss tatsächliche Umsetzung, Verantwortlichkeiten, Intervalle und Nachweise im Kundenblatt bestätigen. Diese Prüffassung behauptet keine bereits nachgewiesene Umsetzung. Nicht zutreffende Maßnahmen sind nachvollziehbar zu begründen; erforderliche Schutzmaßnahmen dürfen nicht ersatzlos entfallen.

C1. Zutritt, Endgeräte und Datenträger

Arbeitsplätze und Datenträger werden vor unberechtigtem Zutritt und Zugriff geschützt. Endgeräte werden gesperrt, aktuell gehalten und angemessen vor Schadsoftware geschützt. Mobile Geräte und Datenträger mit Auftragsdaten werden verschlüsselt. Aufbewahrung, Weitergabe und sichere Löschung sind geregelt; Büro- und Rechenzentrumsmaßnahmen werden getrennt nachgewiesen.

C2. Konten, Berechtigungen und Übertragung

Personenbezogene Administrationskonten, bedarfsgerechte Rechte, sichere Geheimnisverwaltung und geschützte Übertragungswege sind eingerichtet. Privilegierte Zugänge verwenden verfügbare Mehrfaktor-Authentisierung; sonstige Fälle erfordern dokumentierte Ersatzmaßnahmen. Berechtigungen werden regelmäßig und bei Änderungen geprüft. Zugangsdaten gehören nicht in öffentliche Dateien oder Quellcode-Repositories.

C3. Mandantentrennung und Entwicklungsumgebungen

Kundenbestände, Test- und Produktivzugänge werden logisch getrennt. Tests verwenden möglichst synthetische oder wirksam anonymisierte Daten. Erforderliche Echtdatenkopien werden minimiert, dokumentiert, geschützt und nach Zweckerreichung gelöscht. Pseudonymisierung ersetzt nicht die übrigen Schutzmaßnahmen.

C4. Anwendungen, Änderungen und Protokolle

CMS und Extras werden im beauftragten Umfang aktualisiert; Schwachstellen und Supportende werden risikogerecht bearbeitet. Zuständigkeiten und relevante Administrationsvorgänge werden dokumentiert. Protokolle beschränken sich auf Erforderliches; Inhalte, Zugriffe und Löschfristen stehen im Kundenblatt. Formulardaten werden nicht unnötig in Fehlerprotokolle übernommen.

C5. Verfügbarkeit und Wiederherstellung

Sicherungs- und Wiederherstellungsverfahren legen Umfang, Intervall, Aufbewahrung, Speicherort und Verantwortliche fest. Sicherungen werden geschützt, Wiederherstellungen regelmäßig geprüft. Kundenhoster und Agentur-Unterauftragsverarbeiter werden getrennt zugeordnet. Nicht vereinbarte Verfügbarkeit, Wiederanlaufzeiten oder Backup-Produkte werden nicht zugesagt.

C6. Datenminimierung, Löschung und Organisation

Daten und Zugriffe werden auf den Auftrag begrenzt; Löschregeln werden nachweisbar umgesetzt. Für Betroffenenanträge, Vorfälle, Weisungen, Kontrollen und Anbieteränderungen bestehen dokumentierte Zuständigkeiten und erreichbare Kontakte. Vertraulichkeit, Unterweisung und regelmäßige Wirksamkeitskontrolle werden nachgewiesen. Hostingnachweise ersetzen keine Prüfung der Agenturmaßnahmen.

Kundenspezifische Konkretisierung

Das Kundenblatt ergänzt Stand, Zuständigkeiten und Nachweise zu C1–C6. Bei World4You-Einsatz wird dessen konkret datierte Anlage beigelegt. Sicherheitsgeheimnisse, Passwörter, private Mitarbeiteradressen und detaillierte Angriffsflächen gehören nicht in öffentliche Dokumente.

Anlage E – Änderungen und Widersprüche

E1. Mitteilung vor Änderungen

Die Agentur informiert den benannten Empfangskontakt aktiv und nachweisbar vor einer geplanten Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters, einschließlich relevanter Änderungen auf weiteren Stufen. Die Mitteilung nennt mindestens Rechtsträger, Aufgabe, betroffene Daten, Verarbeitungs- und Zugriffsländer, vorgesehenen Beginn sowie maßgebliche Garantien und Übermittlungsgrundlagen. Eine still geänderte Website-Liste genügt nicht.

E2. Vorlauf und Prüfung

Das Kundenblatt legt eine angemessene Mindestvorlauf- und Widerspruchsfrist fest. Die Frist beginnt erst nach Zugang vollständiger Informationen. Sie muss eine sachgerechte Prüfung und einen wirksamen Widerspruch vor dem vorgesehenen Einsatz ermöglichen. Diese Frist ist mit der gesamten Anbieterkette abzugleichen. Solange sie nicht festgelegt ist, ist das Paket nicht abschließbar. Gesetzlich vorgegebene pauschale 14- oder 30-Tage-Fristen bestehen hierfür nicht.

E3. Widerspruch und Lösung

Der Kunde kann innerhalb der vereinbarten Frist unter Angabe nachvollziehbarer datenschutzbezogener Gründe widersprechen. Die Agentur bestätigt den Eingang und klärt die Gründe. Sie prüft zusätzliche Schutzmaßnahmen, einen anderen Anbieter oder eine zumutbare rechtmäßige Fortführung ohne den beanstandeten Dienst. Bis zur Klärung erfolgt keine neue Übermittlung an den beanstandeten Empfänger für diesen Kunden.

Kann keine rechtmäßige und zumutbare Lösung vereinbart werden, können beide Parteien den betroffenen Leistungsteil mit Wirkung vor Beginn des beanstandeten Einsatzes beenden. Migration, Rückgabe und Löschung werden geordnet durchgeführt. Erbrachte Leistungen werden nach Hauptvertrag abgerechnet; das Widerspruchsrecht wird nicht durch eine Vertragsstrafe oder die Zahlung noch nicht erbrachter Restleistungen entwertet. Zwingende Rechte bleiben bestehen.

E4. Kein Widerspruch; dringende Änderungen

Nach fristgerechter vollständiger Mitteilung und Ablauf der vereinbarten Frist ohne Widerspruch darf die Änderung innerhalb der erteilten allgemeinen Genehmigung umgesetzt werden, wenn alle übrigen Voraussetzungen erfüllt sind. Dies ist keine Zustimmung zu neuen AGB, neuen Zwecken, neuen Datenkategorien oder sonstigen Vertragsänderungen.

Dringlichkeit hebt Genehmigungs-, Informations- und Schutzpflichten nicht auf. Ein verkürzter Ablauf bedarf einer ausdrücklichen dokumentierten Zustimmung des Kunden; andernfalls ist die betroffene Verarbeitung gegebenenfalls auszusetzen oder rechtmäßig anderweitig zu erbringen. Eine eigenmächtige Dienstleisteränderung wird nicht durch nachträgliche Information geheilt.

E5. Dokumentation und weitere Änderungen

Mitteilung, Zustellnachweis, Frist, Reaktion, Prüfung, Entscheidung und tatsächlicher Beginn werden dokumentiert. Das Kundenverzeichnis wird versioniert; frühere vereinbarte Fassungen bleiben nachvollziehbar. Kontaktänderungen werden aktiv mitgeteilt. Für geänderte Zwecke, Datenarten, wesentliche Leistungen oder Vertragsklauseln wird eine gesonderte dokumentierte Vereinbarung eingeholt. Rein redaktionelle Korrekturen werden nachvollziehbar dokumentiert und dürfen den Vertragsinhalt nicht verdeckt ändern.