VEREINBARUNG ZUR AUFTRAGSVERARBEITUNG

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)

Allgemeine Fassung der WERTEweb GbR
für die Einbeziehung in Kundenverträge

Veröffentlichungsfassung

Stand: Juli 2026

Diese Vereinbarung zur Auftragsverarbeitung gilt für sämtliche Leistungen der WERTEweb GbR, bei denen personenbezogene Daten im Auftrag eines Kunden verarbeitet werden. Sie wird Bestandteil des jeweiligen Vertragsverhältnisses, sofern im Angebot, Dienstleistungsvertrag oder in den Allgemeinen Geschäftsbedingungen der WERTEweb GbR auf diese AVV Bezug genommen wird. Zu den Leistungen können insbesondere Konzeption, Gestaltung, technische Erstellung, Betrieb, Hosting, Wartung und Weiterentwicklung von Websites und digitalen Anwendungen sowie die Einrichtung von Formularen, Terminbuchungs-, Kommunikations-, Vertriebs-, Marketing-, Automatisierungs- und KI-Lösungen und Supportleistungen gehören.

Diese Vereinbarung konkretisiert die datenschutzrechtlichen Rechte und Pflichten von WERTEweb und dem jeweiligen Kunden nach Art. 28 DSGVO. Bei Widersprüchen zwischen dieser Vereinbarung und dem Hauptvertrag gehen hinsichtlich der Auftragsverarbeitung die Bestimmungen dieser Vereinbarung vor. Wirtschaftliche Leistungs-, Vergütungs- und Haftungsregelungen des Hauptvertrags bleiben im Übrigen unberührt.

§ 1 Gegenstand und Dauer der Verarbeitung

(1) Gegenstand der Auftragsverarbeitung ist die Verarbeitung personenbezogener Daten durch WERTEweb im Zusammenhang mit den im Hauptvertrag, in Leistungsbeschreibungen, Angeboten, Projektbeauftragungen oder dokumentierten Weisungen vereinbarten Leistungen.

(2) Zu den Leistungen können insbesondere gehören: Konzeption, technische Erstellung und Bearbeitung von Websites, Landingpages und Funnels; Einrichtung und Konfiguration von Content-Management-Systemen; Migration von Websites und Daten; Integration von Texten, Bildern und sonstigen Inhalten; technische Implementierung von Formularen, Terminbuchungssystemen, CRM-, Telefonie-, Newsletter-, Chatbot-, KI-, Tracking-, Consent-, Analyse- und Automatisierungslösungen; Schnittstellen- und API-Integrationen; Fehleranalyse und Fehlerbehebung; Hosting, Wartung, Pflege, Weiterentwicklung und Support, soweit jeweils beauftragt.

(3) Art, Umfang, Umstände und Zweck der konkreten Verarbeitung ergeben sich ergänzend aus Anlage 3 sowie aus dem jeweiligen Hauptvertrag, der Projektbeauftragung und den dokumentierten Weisungen des Kunden.

(4) Die Verarbeitung beginnt spätestens mit dem ersten Zugriff von WERTEweb auf personenbezogene Daten und endet, sobald sämtliche Auftragsverarbeitungen beendet und die Daten nach Maßgabe dieser Vereinbarung gelöscht oder zurückgegeben wurden. Für fortlaufende Wartungs-, Hosting- oder Supportleistungen gilt diese Vereinbarung während der gesamten Leistungsdauer.

§ 2 Art und Zweck der Verarbeitung

(1) Die Verarbeitung kann insbesondere das Erheben, Erfassen, Ordnen, Strukturieren, Speichern, Auslesen, Abfragen, Verwenden, Anpassen, Verändern, Übermitteln, Offenlegen durch Übermittlung, Verbreiten oder sonstiges Bereitstellen, Abgleichen, Verknüpfen, Einschränken, Löschen und Vernichten personenbezogener Daten umfassen.

(2) Die Verarbeitung erfolgt ausschließlich zur Erbringung der vertraglich vereinbarten Leistungen und nur im Rahmen der dokumentierten Weisungen des Kunden.

(3) Eine Verarbeitung zu eigenen Zwecken von WERTEweb ist nicht zulässig. Unberührt bleiben Verarbeitungen, für die WERTEweb selbst Verantwortlicher ist, insbesondere die Verarbeitung von Ansprechpartnerdaten zur Vertragsverwaltung, Abrechnung, Erfüllung gesetzlicher Aufbewahrungs- und Nachweispflichten, IT-Sicherheit sowie Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

(4) Soweit einzelne Leistungen keine Auftragsverarbeitung darstellen, insbesondere wenn WERTEweb Zwecke und Mittel einer Verarbeitung eigenständig festlegt, gilt diese Vereinbarung für diese Verarbeitung nicht. Die datenschutzrechtliche Rollenverteilung ist im Zweifel anhand der tatsächlichen Verarbeitung festzustellen.

§ 3 Kategorien betroffener Personen

(1) Abhängig vom jeweiligen Projekt können insbesondere folgende Personengruppen betroffen sein: Kunden und Interessenten des Kunden; Website- und Landingpage-Besucher; Newsletter-Empfänger; Nutzer von Formularen, Chatbots, Terminbuchungs-, Telefonie-, CRM-, Funnel- und Automatisierungssystemen; Ansprechpartner bei Unternehmen; Beschäftigte, Bewerber, freie Mitarbeiter und ehemalige Beschäftigte; Lieferanten, Dienstleister und Geschäftspartner; Teilnehmer von Veranstaltungen oder digitalen Angeboten; sonstige Personen, deren Daten der Kunde in die beauftragten Systeme einstellt.

(2) Die konkret betroffenen Personengruppen werden projektbezogen in Anlage 3 oder einer ergänzenden Leistungsbeschreibung konkretisiert.

§ 4 Kategorien personenbezogener Daten

(1) Abhängig vom jeweiligen Projekt können insbesondere folgende Datenkategorien verarbeitet werden: Stamm- und Kontaktdaten; Unternehmens-, Berufs- und Funktionsdaten; Kommunikations- und Inhaltsdaten; Vertrags-, Kunden-, Interessenten-, Vertriebs- und Vorgangsdaten; Formular-, Termin-, Buchungs- und Kalenderdaten; Telefonie- und Gesprächsmetadaten; Newsletter- und Marketingdaten; Nutzungs-, Geräte-, Browser-, Cookie-, Tracking-, Log- und Zugriffsdaten; IP-Adressen; Support- und Fehlerdaten; Zugangsdaten und technische Identifikatoren; Medien- und Dokumentinhalte; projektbezogen weitere vom Kunden bereitgestellte Daten.

(2) Die Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 DSGVO sowie von Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO ist grundsätzlich nicht Gegenstand der Leistungen.

(3) Sollen solche Daten verarbeitet werden, muss der Kunde dies WERTEweb vor Beginn ausdrücklich mitteilen. WERTEweb und der Kunde vereinbaren vorab die erforderlichen zusätzlichen technischen, organisatorischen und vertraglichen Schutzmaßnahmen. WERTEweb kann die Verarbeitung ablehnen, wenn ein angemessenes Schutzniveau mit vertretbarem Aufwand nicht hergestellt werden kann.

§ 5 Weisungsgebundene Verarbeitung

(1) WERTEweb verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Kunden, es sei denn, WERTEweb ist durch das Recht der Europäischen Union oder eines Mitgliedstaats zu einer Verarbeitung verpflichtet. In diesem Fall teilt WERTEweb dem Kunden diese rechtliche Anforderung vor der Verarbeitung mit, soweit das betreffende Recht eine solche Mitteilung nicht aus wichtigen Gründen des öffentlichen Interesses verbietet.

(2) Weisungen können sich insbesondere aus dem Hauptvertrag, dieser Vereinbarung, Anlage 3, Leistungsbeschreibungen, Projektbeauftragungen, E-Mails, Tickets, Projektmanagement-Systemen oder sonstigen dokumentierten Mitteilungen ergeben.

(3) Mündliche Weisungen sind vom Kunden unverzüglich in Textform zu bestätigen. Weisungsberechtigte Personen können in Anlage 3 oder durch gesonderte Mitteilung benannt werden.

(4) Hält WERTEweb eine Weisung für datenschutzrechtswidrig, informiert WERTEweb den Kunden unverzüglich. WERTEweb ist berechtigt, die betreffende Verarbeitung bis zur Bestätigung, Änderung oder Klärung der Weisung auszusetzen, soweit dies zur Vermeidung eines Datenschutzverstoßes erforderlich ist.

(5) WERTEweb schuldet keine umfassende rechtliche Prüfung der Weisungen oder der vom Kunden eingesetzten Inhalte, Einwilligungstexte, Datenschutzerklärungen oder Rechtsgrundlagen, sofern dies nicht ausdrücklich als gesonderte Beratungsleistung vereinbart wurde.

§ 6 Pflichten und Verantwortlichkeit des Kunden

(1) Der Kunde ist für die Rechtmäßigkeit der Verarbeitung, die Zulässigkeit der Übermittlung an WERTEweb und die Rechtmäßigkeit seiner Weisungen verantwortlich.

(2) Der Kunde gewährleistet insbesondere, dass geeignete Rechtsgrundlagen bestehen, Informationspflichten erfüllt werden, erforderliche Einwilligungen wirksam eingeholt und nachweisbar dokumentiert werden, die Grundsätze des Art. 5 DSGVO eingehalten werden und nur erforderliche Daten verarbeitet werden.

(3) Der Kunde informiert WERTEweb rechtzeitig über besondere Risiken, besondere Datenkategorien, gesetzliche Geheimhaltungspflichten, branchenspezifische Anforderungen, Löschfristen und sonstige Umstände, die für eine rechtmäßige und sichere Verarbeitung erheblich sind.

(4) Der Kunde verwaltet seine eigenen Nutzerkonten, Rollen und Berechtigungen sachgerecht, soweit dies in seinem Verantwortungsbereich liegt. Er schützt Zugangsdaten, aktiviert verfügbare Mehrfaktor-Authentifizierung und entzieht nicht mehr benötigte Berechtigungen unverzüglich.

(5) Soweit der Kunde selbst Auftragsverarbeiter eines Dritten ist, gewährleistet er, dass er zum Einsatz von WERTEweb als weiterem Auftragsverarbeiter berechtigt ist und die Weisungen des Verantwortlichen einhält.

§ 7 Pflichten von WERTEweb und Vertraulichkeit

(1) WERTEweb verarbeitet personenbezogene Daten ausschließlich im Rahmen dieser Vereinbarung und der dokumentierten Weisungen des Kunden.

(2) WERTEweb gewährleistet, dass zur Verarbeitung befugte Personen personenbezogene Daten nur im Rahmen der ihnen übertragenen Aufgaben verarbeiten, zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und über die wesentlichen datenschutzrechtlichen und sicherheitsbezogenen Anforderungen informiert wurden.

(3) WERTEweb beschränkt den Zugriff auf personenbezogene Daten auf Personen, die ihn zur Erbringung der Leistungen benötigen. Administrations- und Supportzugriffe erfolgen nur soweit erforderlich und werden nach Möglichkeit zeitlich und sachlich beschränkt.

(4) WERTEweb führt ein Verzeichnis der für WERTEweb einschlägigen Verarbeitungstätigkeiten nach Maßgabe des Art. 30 Abs. 2 DSGVO und arbeitet mit der zuständigen Aufsichtsbehörde zusammen, soweit dies gesetzlich erforderlich ist.

(5) WERTEweb bestellt einen Datenschutzbeauftragten, soweit die gesetzlichen Voraussetzungen hierfür vorliegen, und teilt dessen Kontaktdaten dem Kunden auf Anfrage mit.

§ 8 Technische und organisatorische Maßnahmen

(1) WERTEweb trifft unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken angemessene technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO.

(2) Die bei Abschluss dieser Vereinbarung vereinbarten Maßnahmen ergeben sich aus Anlage 1. Sie bilden ein dem jeweiligen Risiko angemessenes Schutzniveau ab.

(3) WERTEweb darf die Maßnahmen an technische, organisatorische oder rechtliche Entwicklungen anpassen, sofern das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen, die das Schutzniveau betreffen, werden dokumentiert.

(4) Soweit der Kunde Systeme, Hostingumgebungen, Accounts, Plugins, Schnittstellen oder Zugangsmethoden vorgibt oder bereitstellt, bleibt er für deren sichere Grundkonfiguration und die ihm zugewiesenen Verantwortungsbereiche verantwortlich. WERTEweb weist auf erkennbare erhebliche Sicherheitsrisiken hin.

§ 9 Unterstützung bei Betroffenenrechten

(1) WERTEweb unterstützt den Kunden unter Berücksichtigung der Art der Verarbeitung und der verfügbaren Informationen durch geeignete technische und organisatorische Maßnahmen dabei, Anträge betroffener Personen auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch zu erfüllen.

(2) Wendet sich eine betroffene Person unmittelbar an WERTEweb, beantwortet WERTEweb die Anfrage grundsätzlich nicht eigenständig, sondern leitet sie unverzüglich an den Kunden weiter, sofern keine gesetzliche Verpflichtung zu einer unmittelbaren Antwort besteht.

(3) Der Kunde erteilt die für die Bearbeitung erforderlichen Weisungen und entscheidet über die rechtliche Zulässigkeit und den Umfang der Antwort.

(4) Unterstützungsleistungen, die über den typischen und ohne nennenswerten Zusatzaufwand möglichen Umfang hinausgehen, können nach dem vereinbarten Stundensatz vergütet werden. Dies gilt nicht, soweit der Unterstützungsbedarf auf einer von WERTEweb schuldhaft verursachten Vertrags- oder Datenschutzverletzung beruht.

§ 10 Unterstützung bei Sicherheit, Folgenabschätzung und Behörden

(1) WERTEweb unterstützt den Kunden unter Berücksichtigung der Art der Verarbeitung und der verfügbaren Informationen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO, insbesondere bei der Bewertung von Sicherheitsmaßnahmen, Datenschutz-Folgenabschätzungen und vorherigen Konsultationen.

(2) Die Verantwortung für die Durchführung und Dokumentation einer Datenschutz-Folgenabschätzung sowie für die Entscheidung über eine Konsultation der Aufsichtsbehörde verbleibt beim Kunde, soweit dieser Verantwortlicher ist.

(3) WERTEweb stellt auf Anfrage die in seinem Verantwortungsbereich vorhandenen Informationen bereit, soweit dadurch keine Rechte Dritter, Geschäftsgeheimnisse oder Sicherheitsinteressen unangemessen beeinträchtigt werden.

§ 11 Meldung von Datenschutzverletzungen

(1) WERTEweb informiert den Kunden unverzüglich, nachdem WERTEweb eine Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit der Auftragsverarbeitung bekannt geworden ist.

(2) Die Mitteilung enthält, soweit verfügbar, eine Beschreibung der Art der Verletzung, betroffene Datenkategorien und Personengruppen, soweit möglich die ungefähre Anzahl betroffener Personen und Datensätze, wahrscheinliche Folgen, bereits ergriffene oder vorgeschlagene Abhilfemaßnahmen sowie eine Kontaktstelle für Rückfragen.

(3) Können Informationen nicht gleichzeitig bereitgestellt werden, dürfen sie ohne unangemessene weitere Verzögerung schrittweise übermittelt werden.

(4) WERTEweb trifft unverzüglich angemessene Maßnahmen zur Eindämmung, Behebung und Untersuchung des Vorfalls, soweit dieser in seinem Verantwortungsbereich liegt, und unterstützt den Kunden bei erforderlichen Meldungen und Benachrichtigungen.

(5) Die Mitteilung eines Vorfalls stellt kein Anerkenntnis einer rechtlichen Verantwortlichkeit oder eines Verschuldens dar. Die Entscheidung über Meldungen nach Art. 33 DSGVO und Benachrichtigungen nach Art. 34 DSGVO obliegt dem Kunden, soweit er Verantwortlicher ist.

§ 12 Weitere Auftragsverarbeiter

(1) Der Kunde erteilt WERTEweb die allgemeine schriftliche Genehmigung, weitere Auftragsverarbeiter einzusetzen, soweit dies zur Erbringung der Leistungen erforderlich ist.

(2) Die bei Abschluss dieser Vereinbarung regelmäßig oder projektbezogen eingesetzten weiteren Auftragsverarbeiter sind in Anlage 2 aufgeführt. Ein Dienstleister ist nur insoweit weiterer Auftragsverarbeiter, als er tatsächlich personenbezogene Daten im Auftrag verarbeitet.

(3) WERTEweb informiert den Kunden über beabsichtigte Änderungen hinsichtlich der Hinzuziehung oder Ersetzung weiterer Auftragsverarbeiter. Die Information kann per E-Mail, Kundenportal oder durch Bereitstellung einer aktualisierten Liste erfolgen.

(4) Der Kunde kann aus wichtigem datenschutzrechtlichem Grund innerhalb von 14 Kalendertagen nach Zugang der Information widersprechen. Im Fall eines begründeten Widerspruchs bemühen sich WERTEweb und der Kunde um eine angemessene Alternative. Ist eine Alternative nicht möglich oder wirtschaftlich unzumutbar, kann die von der Änderung betroffene Leistung beendet werden.

(5) WERTEweb verpflichtet weitere Auftragsverarbeiter vertraglich im Wesentlichen zu denselben Datenschutzpflichten, die WERTEweb nach dieser Vereinbarung obliegen. WERTEweb bleibt gegenüber dem Kunden nach Maßgabe der gesetzlichen Vorschriften für die Erfüllung der Pflichten des weiteren Auftragsverarbeiters verantwortlich.

(6) Der Kunde erkennt an, dass bei projektbezogenen Kundensystemen auch solche Anbieter eingesetzt werden können, die der Kunde selbst auswählt, beauftragt oder administriert. WERTEweb und der Kunde dokumentieren in diesem Fall die jeweilige Rollen- und Verantwortungsverteilung.

§ 13 Verarbeitung in Drittländern

(1) Eine Verarbeitung personenbezogener Daten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

(2) Als Übermittlungsgrundlage können insbesondere ein Angemessenheitsbeschluss der Europäischen Kommission, einschließlich einer anwendbaren und gültigen Zertifizierung unter dem EU-US Data Privacy Framework, die Standardvertragsklauseln der Europäischen Kommission oder ein anderes gesetzlich anerkanntes Übermittlungsinstrument dienen.

(3) Soweit erforderlich, werden eine Transfer Impact Assessment und ergänzende technische, organisatorische oder vertragliche Schutzmaßnahmen umgesetzt. Die konkrete Übermittlungsgrundlage eines Anbieters richtet sich nach dem zum Zeitpunkt der Verarbeitung gültigen Status und den mit dem Anbieter geschlossenen Vertragsunterlagen.

(4) Die Aufnahme eines US-Anbieters in Anlage 2 stellt keine Zusicherung dar, dass dieser Anbieter zu jedem Zeitpunkt unter dem EU-US Data Privacy Framework zertifiziert ist. WERTEweb prüft beziehungsweise dokumentiert für den tatsächlichen Einsatz eine zulässige Übermittlungsgrundlage.

§ 14 Hosting, Administrations- und Supportzugriffe

(1) Soweit Hosting, Betrieb, Wartung oder Support beauftragt sind, darf WERTEweb im erforderlichen Umfang auf produktive Systeme, Datenbanken, Protokolle, Backups und Administrationsoberflächen zugreifen.

(2) Zugriffe erfolgen ausschließlich zur Erbringung der beauftragten Leistungen, zur Fehleranalyse, Wiederherstellung, Absicherung, Aktualisierung oder technischen Optimierung und werden auf das notwendige Maß beschränkt.

(3) Zugangsdaten werden nach Möglichkeit über geeignete Passwortmanager oder andere geschützte Übermittlungswege verwaltet. Eine ungeschützte Übermittlung sensibler Zugangsdaten soll vermieden werden.

(4) Soweit WERTEweb keinen Einfluss auf Hostinganbieter, Serverkonfiguration, Backupzyklen oder Kundensysteme hat, richtet sich die Verantwortlichkeit nach dem Hauptvertrag und der tatsächlichen Zugriffsmöglichkeit. WERTEweb schuldet nur ausdrücklich beauftragte Backup-, Monitoring- oder Wiederherstellungsleistungen.

§ 15 Cloud-, Automatisierungs-, Kommunikations- und KI-Dienste

(1) WERTEweb darf im Rahmen der genehmigten weiteren Auftragsverarbeiter cloudbasierte Dienste, Automatisierungsplattformen, Terminbuchungs-, Funnel-, CRM-, Telefonie-, Kommunikations- und KI-Systeme einsetzen, soweit dies zur Vertragserfüllung erforderlich ist.

(2) Personenbezogene Daten dürfen nur in dem für den jeweiligen Zweck erforderlichen Umfang an solche Systeme übermittelt werden. Soweit technisch und sachlich möglich, werden Daten minimiert, pseudonymisiert oder von unmittelbar identifizierenden Angaben befreit.

(3) Bei KI-Diensten werden personenbezogene Daten nur verarbeitet, wenn dies projektbezogen vereinbart oder für die beauftragte Funktion erforderlich ist. WERTEweb nutzt verfügbare Einstellungen zur Beschränkung einer Nutzung zu Trainings- oder eigenen Anbieterzwecken, soweit diese für das eingesetzte Produkt verfügbar und vertraglich zugesichert sind.

(4) Der Kunde darf keine besonders sensiblen Daten, Berufsgeheimnisse oder besonderen Kategorien personenbezogener Daten in cloudbasierte oder KI-Systeme einstellen lassen, sofern dies nicht ausdrücklich vereinbart und durch angemessene Schutzmaßnahmen abgesichert wurde.

(5) Die Auswahl und Konfiguration projektbezogener Systeme wird in Anlage 2 und Anlage 3 oder einer ergänzenden Projektbeschreibung dokumentiert.

§ 16 Kontroll- und Nachweisrechte

(1) WERTEweb stellt dem Kunden alle Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der Pflichten aus Art. 28 DSGVO nachzuweisen.

(2) Der Nachweis kann insbesondere durch Auskünfte, Dokumentationen, Selbstauskünfte, Datenschutz- und Sicherheitskonzepte, Zertifikate, Prüfberichte oder sonstige geeignete Nachweise erfolgen.

(3) Soweit diese Nachweise zur Beurteilung nicht ausreichen, ist der Kunde berechtigt, nach angemessener vorheriger Ankündigung eine Kontrolle selbst oder durch einen unabhängigen, sachkundigen und zur Vertraulichkeit verpflichteten Dritten durchführen zu lassen.

(4) Kontrollen sind grundsätzlich während der üblichen Geschäftszeiten, mit angemessener Vorankündigung und unter Rücksichtnahme auf den Geschäftsbetrieb, Sicherheitsinteressen, Rechte anderer Kunden und Geschäftsgeheimnisse durchzuführen. Direkte Zugriffe auf Systeme anderer Kunden sind ausgeschlossen.

(5) Der Kunde trägt die angemessenen Kosten einer Kontrolle, sofern die Kontrolle nicht einen erheblichen von WERTEweb zu vertretenden Verstoß ergibt oder gesetzlich etwas anderes vorgesehen ist. Wiederholte Kontrollen ohne konkreten Anlass können nach Aufwand vergütet werden.

§ 17 Rückgabe und Löschung personenbezogener Daten

(1) Nach Abschluss der Verarbeitung löscht oder übergibt WERTEweb nach Wahl und Weisung des Kunden die im Auftrag verarbeiteten personenbezogenen Daten und vorhandenen Kopien, soweit keine gesetzliche Verpflichtung zur weiteren Speicherung besteht.

(2) Die Löschung erfolgt innerhalb einer angemessenen Frist unter Berücksichtigung technischer Abläufe, vertraglicher Übergaben, offener Supportfälle und vereinbarter Aufbewahrungs- oder Migrationszeiträume.

(3) Daten in Sicherungskopien und Backups dürfen im Rahmen regulärer Lösch- und Überschreibungszyklen gelöscht werden, sofern sie bis zur endgültigen Löschung nicht für andere Zwecke verarbeitet werden und angemessenen Schutzmaßnahmen unterliegen.

(4) Gesetzliche Aufbewahrungs-, Dokumentations- und Nachweispflichten von WERTEweb bleiben unberührt. In diesem Fall werden die Daten für andere Zwecke gesperrt beziehungsweise nur noch zur Erfüllung der gesetzlichen Pflicht verarbeitet.

(5) Zugangsdaten, lokale Arbeitskopien und temporäre Exportdateien werden nach Wegfall ihrer Erforderlichkeit gelöscht oder unbrauchbar gemacht, soweit keine berechtigte weitere Speicherung besteht.

§ 18 Haftung und Freistellung

(1) Für die Haftung der Parteien gelten die gesetzlichen Bestimmungen, insbesondere Art. 82 DSGVO, sowie ergänzend die wirksamen Haftungsregelungen des Hauptvertrags.

(2) WERTEweb und der Kunde unterstützen sich gegenseitig bei der Aufklärung datenschutzrechtlicher Schadensfälle und stellen einander die im jeweiligen Verantwortungsbereich verfügbaren Informationen zur Verfügung.

(3) Soweit WERTEweb oder der Kunde einen Schaden oder Datenschutzverstoß allein zu vertreten hat, trägt sie die daraus entstehenden Verantwortlichkeiten und Kosten nach Maßgabe

der gesetzlichen Vorschriften. Bei gemeinsamer Verantwortlichkeit richtet sich die interne Verteilung nach dem jeweiligen Anteil an der Verursachung und Verantwortung.

(4) Der Kunde stellt WERTEweb von Ansprüchen frei, die auf rechtswidrigen Weisungen, unzulässigen Inhalten, fehlenden Rechtsgrundlagen oder Pflichtverletzungen im Verantwortungsbereich des Kunden beruhen, soweit WERTEweb den zugrunde liegenden Umstand nicht mitverursacht hat und die Freistellung rechtlich zulässig ist.

§ 19 Laufzeit und Beendigung

(1) Diese Vereinbarung tritt mit ihrer wirksamen Einbeziehung in den jeweiligen Hauptvertrag, spätestens jedoch mit Beginn der ersten Auftragsverarbeitung, in Kraft.

(2) Sie gilt für die Dauer sämtlicher Verarbeitungen personenbezogener Daten durch WERTEweb im Auftrag des Kunden. Eine gesonderte ordentliche Kündigung ist während einer laufenden Auftragsverarbeitung ausgeschlossen.

(3) Die Vereinbarung endet, wenn sämtliche Auftragsverarbeitungen beendet, personenbezogene Daten nach Maßgabe dieser Vereinbarung gelöscht oder zurückgegeben und keine gesetzlichen Verpflichtungen zur weiteren Speicherung mehr bestehen.

(4) Vertraulichkeits-, Nachweis-, Lösch- und sonstige Pflichten, die ihrer Natur nach über die Vertragsbeendigung hinaus gelten, bleiben unberührt.

§ 20 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform, soweit gesetzlich keine strengere Form vorgeschrieben ist. Dies gilt auch für Änderungen der Anlagen.

(2) Sollte eine Bestimmung dieser Vereinbarung ganz oder teilweise unwirksam oder undurchführbar sein oder werden, bleiben die übrigen Bestimmungen unberührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung treten die gesetzlichen Vorschriften.

(3) Es gilt deutsches Recht. Gerichtsstandsregelungen richten sich nach dem Hauptvertrag und den gesetzlichen Vorschriften.

(4) Die Anlagen 1 bis 3 sind Bestandteil dieser Vereinbarung. Projektbezogene Ergänzungen können in Textform vereinbart werden.

ANLAGE 1

Technische und organisatorische Maßnahmen (TOMs) gemäß Art. 32 DSGVO

Die folgenden Maßnahmen beschreiben das grundsätzlich vereinbarte Schutzniveau. Die konkret erforderlichen Maßnahmen richten sich nach Art, Umfang, Umständen und Zweck der jeweiligen Verarbeitung sowie den Risiken für die Rechte und Freiheiten natürlicher Personen. Maßnahmen, die technisch nicht einschlägig sind oder außerhalb des Verantwortungsbereichs von WERTEweb liegen, werden nur angewendet, soweit dies projektbezogen vereinbart ist.

1. Organisation des Datenschutzes

- Benennung klarer Verantwortlichkeiten für Datenschutz und Informationssicherheit.
- Dokumentierte Verpflichtung befugter Personen auf Vertraulichkeit.
- Anlassbezogene Sensibilisierung zu Datenschutz, Phishing, Zugangsschutz und sicherem Umgang mit Kundendaten.
- Dokumentierte Auswahl und vertragliche Einbindung von Auftragsverarbeitern.
- Verfahren zur regelmäßigen Überprüfung und Anpassung der Maßnahmen.

2. Zutrittskontrolle

- Angemessene Sicherung von Büroräumen und häuslichen Arbeitsbereichen gegen unbefugten Zutritt.
- Kontrollierter Umgang mit Schlüsseln, Schließsystemen und sonstigen Zugangsmöglichkeiten.
- Arbeitsgeräte werden nicht unbeaufsichtigt in frei zugänglichen Bereichen zurückgelassen.
- Papierunterlagen mit personenbezogenen Daten werden, soweit vorhanden, sicher verwahrt und datenschutzgerecht vernichtet.
- Mobile Arbeitsplätze werden so gewählt und organisiert, dass eine Kenntnisnahme durch Unbefugte vermieden wird.

3. Zugangskontrolle

- Verwendung individueller Benutzerkonten; keine gemeinsame Nutzung administrativer Konten, soweit technisch vermeidbar.
- Starke, individuelle Passwörter und Nutzung eines geeigneten Passwortmanagers.
- Mehrfaktor-Authentifizierung für zentrale, administrative und cloudbasierte Dienste, soweit technisch verfügbar und angemessen.
- Automatische oder manuelle Bildschirmsperre bei Nichtbenutzung.
- Sichere Wiederherstellungs- und Notfallzugänge; regelmäßige Überprüfung nicht mehr benötigter Accounts.
- Schutz vor Brute-Force-Angriffen und missbräuchlichen Anmeldeversuchen, soweit durch das jeweilige System unterstützt.

4. Zugriffskontrolle und Berechtigungsmanagement

- Rollen-, projekt- und aufgabenbezogene Vergabe von Zugriffsrechten nach dem Need-to-know- und Least-Privilege-Prinzip.
- Beschränkung administrativer Rechte auf das erforderliche Maß.
- Unverzügliche Anpassung oder Entfernung von Berechtigungen bei Aufgabenwechsel oder Projektende.
- Trennung von Kunden- und Projektzugängen, soweit technisch und organisatorisch möglich.
- Regelmäßige Überprüfung privilegierter Zugänge und externer Freigaben.

- Keine Nutzung von Kundendaten zu privaten oder nicht beauftragten Zwecken.

5. Weitergabekontrolle und Übertragungssicherheit

- Nutzung verschlüsselter Verbindungen nach dem Stand der Technik, insbesondere TLS/HTTPS.
- Nutzung sicherer Dateiübertragungs-, Cloud- oder Projektplattformen.
- Vermeidung ungeschützter Übermittlung von Passwörtern, API-Schlüsseln und sonstigen Zugangsdaten.
- Getrennte Übermittlung besonders schutzbedürftiger Zugangsinformationen, soweit angemessen.
- Prüfung von Empfängern und Berechtigungen vor Freigaben oder Übermittlungen.
- Datenminimierung bei Exporten, Supportzugriffen und Übermittlungen an weitere Auftragsverarbeiter.

6. Eingabekontrolle und Nachvollziehbarkeit

- Nutzung von Benutzerkonten, Systemlogs, Versionshistorien, Änderungsprotokollen und Ticketverläufen, soweit im jeweiligen System verfügbar.
- Dokumentation wesentlicher administrativer Änderungen und Weisungen über geeignete Projekt- oder Kommunikationssysteme.
- Zeitliche Begrenzung und Deaktivierung temporärer Supportzugänge nach Abschluss der Tätigkeit.
- Protokolldaten werden nur im erforderlichen Umfang und für angemessene Zeiträume vorgehalten.

7. Auftragskontrolle

- Abschluss und Pflege von Vereinbarungen zur Auftragsverarbeitung.
- Dokumentierte Annahme, Prüfung und Umsetzung von Weisungen.
- Sorgfältige Auswahl und regelmäßige Überprüfung wesentlicher Dienstleister.
- Vertragliche Verpflichtung weiterer Auftragsverarbeiter auf angemessene Datenschutz- und Sicherheitsstandards.
- Klare Abgrenzung der Verantwortlichkeiten bei kundenseitig bereitgestellten Systemen und Accounts.

8. Verfügbarkeitskontrolle und Belastbarkeit

- Nutzung angemessen geschützter IT-, Hosting- und Cloud-Systeme.
- Regelmäßige Installation sicherheitsrelevanter Updates für Betriebssysteme, Browser, Plugins und Anwendungen.
- Angemessener Schutz vor Schadsoftware, Phishing und bekannten Angriffsmustern.
- Datensicherung und Wiederherstellung, soweit dies zum beauftragten Verantwortungsbereich von WERTEweb gehört.
- Nutzung redundanter oder hochverfügbarer Dienstleister, soweit vertraglich vereinbart.
- Notfallkontakte und Verfahren zur Reaktion auf Ausfälle und Sicherheitsvorfälle.

9. Trennungsgebot

- Logische Trennung von Daten verschiedener Kunden und Projekte.
- Getrennte Kundenkonten, Mandanten, Projektbereiche, Verzeichnisse oder Ablagestrukturen, soweit technisch möglich.
- Rollenbasierte Berechtigungen und getrennte Zugangsdaten.
- Trennung von Test- und Produktivumgebungen, soweit projektbezogen vorgesehen.
- Vermeidung der Verwendung realer personenbezogener Daten in Testsystemen, soweit dies nicht erforderlich ist.

10. Schutz der Arbeitsgeräte

- Verwendung unterstützter und aktuell gehaltener Betriebssysteme.
- Regelmäßige Sicherheitsupdates für Endgeräte und eingesetzte Anwendungen.
- Geräte- und Bildschirmsperren sowie Passwort- oder biometrischer Schutz.
- Verschlüsselung mobiler Arbeitsgeräte und Datenträger, soweit technisch verfügbar und angemessen.
- Keine unkontrollierte Nutzung privater oder fremder Datenträger für Kundendaten.
- Angemessene Fernlösch-, Wiederherstellungs- oder Sperrmöglichkeiten, soweit verfügbar.

11. Passwort- und Geheimnismanagement

- Verwendung sicherer und individueller Passwörter.
- Nutzung eines Passwortmanagers für projekt- und kundenbezogene Zugänge.
- Keine unbefugte Weitergabe von Passwörtern, API-Schlüsseln, Tokens oder Wiederherstellungscodes.
- Änderung oder Sperrung von Zugangsdaten bei Verdacht auf Kompromittierung.
- Beschränkung und regelmäßige Rotation besonders privilegierter Geheimnisse, soweit technisch und projektbezogen angemessen.

12. Sichere Entwicklung und Systemkonfiguration

- Berücksichtigung datenschutzfreundlicher Voreinstellungen, soweit WERTEweb Einfluss auf die Konfiguration hat und entsprechende Weisungen vorliegen.
- Beschränkung nicht benötigter Dienste, Plugins, Schnittstellen und Berechtigungen.
- Installation von Sicherheitsupdates und Entfernung nicht mehr benötigter Komponenten im vereinbarten Wartungsumfang.
- Prüfung von Formularen, Zugriffsrechten und Datenflüssen im Rahmen des beauftragten Leistungsumfangs.
- Keine Garantie für absolute Fehler- oder Angriffsfreiheit; Maßnahmen werden risikoorientiert nach dem Stand der Technik umgesetzt.

13. Backup und Wiederherstellung

- Festlegung von Backupumfang, Frequenz, Aufbewahrung und Wiederherstellung im Hauptvertrag oder Projektauftrag, soweit WERTEweb hierfür verantwortlich ist.
- Backups werden vor unbefugtem Zugriff geschützt und nach Möglichkeit getrennt von Produktivsystemen gespeichert.
- Wiederherstellungsmöglichkeiten werden risikoorientiert oder im vereinbarten Umfang getestet.
- Backups werden nach festgelegten Zyklen überschrieben oder gelöscht.
- Bei kundenseitig verantworteten Hostingumgebungen obliegt die Prüfung und Beauftragung geeigneter Backups dem Kunden, sofern nichts anderes vereinbart ist.

14. Verfahren bei Datenschutzverletzungen

- Zentrale und unverzügliche Aufnahme bekannt gewordener Sicherheitsvorfälle.
- Bewertung der betroffenen Systeme, Daten, Personen und möglichen Auswirkungen.
- Einleitung geeigneter Eindämmungs-, Sicherungs- und Abhilfemaßnahmen.
- Dokumentation relevanter Fakten, Maßnahmen und Zeitpunkte.
- Unverzügliche Information des Kunden gemäß § 11 der Vereinbarung.
- Nachbereitung und Anpassung von Maßnahmen, soweit erforderlich.

15. Löschung und Datenträgerentsorgung

- Projektbezogene Löschung lokaler Kopien und temporärer Exporte nach Wegfall der Erforderlichkeit.
- Löschung oder Rückgabe bei Vertragsende nach Weisung des Kunden.
- Datenschutzgerechte Löschung, Überschreibung oder physische Vernichtung von Datenträgern, soweit erforderlich.
- Berücksichtigung regulärer Backup- und Archivzyklen.
- Sperrung von Daten, die aufgrund gesetzlicher Pflichten weiter aufbewahrt werden müssen.

16. Homeoffice und mobiles Arbeiten

- Verarbeitung nur über angemessen geschützte Arbeitsgeräte und Verbindungen.
- Vermeidung von Einsichtnahme oder Mithören durch Haushaltsangehörige und Dritte.
- Nutzung von Sichtschutz, Headsets oder geeigneter räumlicher Trennung, soweit erforderlich.
- Keine dauerhafte ungeschützte Ablage personenbezogener Daten auf privaten Endgeräten oder Papierunterlagen.
- Sichere Aufbewahrung von Arbeitsgeräten außerhalb der Nutzungszeiten.

17. Regelmäßige Überprüfung

- Überprüfung der technischen und organisatorischen Maßnahmen in angemessenen Abständen sowie bei wesentlichen Änderungen der Verarbeitung oder Systeme.
- Berücksichtigung bekannt gewordener Schwachstellen, Vorfälle, neuer Angriffsmethoden und technischer Entwicklungen.
- Anpassung von Zugängen, Berechtigungen und Dienstleistern bei Projekt- oder Personaländerungen.
- Dokumentation wesentlicher Änderungen am Schutzniveau.

ANLAGE 2

Genehmigte weitere Auftragsverarbeiter

Die nachstehende Liste enthält Anbieter, die abhängig vom jeweiligen Projekt und Leistungsumfang eingesetzt werden können. Nicht jeder Anbieter wird in jedem Projekt eingesetzt. Die konkrete Auswahl wird durch Angebot, Leistungsbeschreibung, Projektkonfiguration oder Weisung bestimmt. Vor dem tatsächlichen Einsatz ist zu prüfen, ob ein AV-Verhältnis besteht und welche aktuelle Übermittlungsgrundlage gilt.

Anbieter / mögliche Vertragsgesellschaft	Zweck	Sitz / Verarbeitungsregion	Drittlandtransfer	Übermittlungs- / Vertragsgrundlage
Hostinganbieter des jeweiligen Projekts (z. B. Hetzner Online GmbH, IONOS SE, ALL-INKL.COM – Neue Medien Münnich)	Hosting, Server, Domains, Backups, technische Infrastruktur	Deutschland / EU je nach Anbieter	regelmäßig nein; abhängig von Konfiguration	Art. 28 DSGVO; projektbezogene Auswahl
Cloudflare, Inc.	DNS, CDN, Web-Sicherheit, DDoS-Schutz, Performance	USA / internationale Infrastruktur	möglich	Angemessenheitsbeschluss/DPF, soweit anwendbar, oder SCC und ergänzende Maßnahmen
OpenAI, L.L.C. bzw. zuständige OpenAI-Vertragsgesellschaft	KI-Funktionen, API, Chatbot- und Automatisierungsleistungen	USA / ggf. weitere Regionen	möglich	DPF, soweit gültig und anwendbar, oder SCC; konkrete Produkt- und Vertragsprüfung
Anthropic, PBC bzw. zuständige Vertragsgesellschaft	KI-Funktionen und API-Leistungen	USA	möglich	SCC oder andere gültige Übermittlungsgrundlage; konkrete Vertragsprüfung
Microsoft Ireland Operations Ltd. / Microsoft Corporation	Microsoft 365, E-Mail, Dokumente, Cloud- und Kollaborationsdienste	Irland / USA / internationale Infrastruktur	möglich	Art. 28 DSGVO; DPF oder SCC, soweit erforderlich
Google Ireland Ltd. / Google LLC	Google Workspace, Kalender, Cloud- und Integrationsdienste	Irland / USA / internationale Infrastruktur	möglich	Art. 28 DSGVO; DPF oder SCC, soweit erforderlich
Brevo (Sendinblue GmbH bzw. zuständige Gesellschaft)	E-Mail-Versand, Newsletter, Marketing-Automation	Deutschland / EU	grundsätzlich nein, abhängig von Subdienstleistern	Art. 28 DSGVO; ggf. Art. 44 ff. DSGVO für Subdienstleister
Make / Celonis, Inc. bzw. zuständige Make-Vertragsgesellschaft	Workflow- und Datenautomatisierung, Schnittstellen	EU / USA je nach Vertrags- und Hostingmodell	möglich	Art. 28 DSGVO; DPF oder SCC, soweit erforderlich
Zapier, Inc.	Workflow- und Datenautomatisierung	USA	ja/möglich	DPF, soweit anwendbar, oder SCC und ergänzende Maßnahmen
Focus.Dialer – konkrete Vertragsgesellschaft gemäß Kundenkonto	Telefonie, Vertriebs- und Kommunikationsprozesse, CRM-nahe Funktionen	USA (nach Angabe des WERTEwebs)	ja/möglich	DPF, sofern Anbieter und Produkt gültig zertifiziert, andernfalls SCC und ergänzende Maßnahmen
Funnel.Page – konkrete Vertragsgesellschaft gemäß Kundenkonto	Landingpages, Funnels, Formulare, Lead- und Conversion-Prozesse	USA (nach Angabe des WERTEwebs)	ja/möglich	DPF, sofern Anbieter und Produkt gültig zertifiziert, andernfalls SCC und ergänzende Maßnahmen
Zeeg GmbH bzw. zuständige Vertragsgesellschaft	Terminbuchung, Kalenderkoordination und Integrationen	Deutschland / EU nach Anbieterangaben	grundsätzlich nein; abhängig von Subdienstleistern	Art. 28 DSGVO; ggf. Art. 44 ff. DSGVO für Subdienstleister
Calendly, LLC	Terminbuchung und Kalenderintegration	USA	ja/möglich	DPF, soweit anwendbar, oder SCC und ergänzende Maßnahmen
Projektbezogene Freelancer und technische Spezialisten	Entwicklung, Design, Wartung, Support oder Migration	Deutschland / EU, sofern nicht anders mitgeteilt	grundsätzlich nein	Unterauftragsverarbeitungsvertrag gemäß Art. 28 Abs. 4 DSGVO

Hinweis: Marken- und Produktnamen können von den jeweiligen rechtlichen Vertragsgesellschaften abweichen. Für den produktiven Einsatz sind die im Kundenkonto, Auftragsformular oder AV-Vertrag genannten juristischen Personen maßgeblich. WERTEweb darf die Liste nach § 12 aktualisieren.

ANLAGE 3

Allgemeine Beschreibung der Auftragsverarbeitung

Diese Anlage beschreibt den typischen Rahmen der Verarbeitung bei Leistungen der WERTEweb GbR. Die konkrete Ausgestaltung ergibt sich ergänzend aus dem jeweiligen Angebot, Hauptvertrag, der Leistungsbeschreibung, der Projektkonfiguration und dokumentierten Weisungen des Kunden. Nicht jede der nachfolgend beschriebenen Verarbeitungstätigkeiten findet in jedem Projekt statt.

1. Gegenstand der Verarbeitung

Gegenstand ist die technische, organisatorische und gestalterische Erbringung digitaler Leistungen. Hierzu können insbesondere Websites, Landingpages, Funnels, Formulare, Terminbuchungs-, Newsletter-, CRM-, Telefonie-, Automatisierungs-, Chatbot- und KI-Systeme sowie Hosting-, Wartungs-, Support-, Migrations- und Integrationsleistungen gehören.

2. Zwecke der Verarbeitung

Die Verarbeitung dient ausschließlich der Erbringung, Absicherung, Wartung, Fehleranalyse, Optimierung und Dokumentation der beauftragten Leistungen. Eine Verarbeitung durch WERTEweb für eigene Werbe-, Profilbildungs- oder sonstige vertragsfremde Zwecke findet im Rahmen dieser AVV nicht statt.

3. Typische Verarbeitungsvorgänge

Je nach Projekt können Daten erhoben, erfasst, geordnet, strukturiert, gespeichert, ausgelesen, abgefragt, verwendet, angepasst, verändert, übermittelt, bereitgestellt, abgeglichen, verknüpft, eingeschränkt, gelöscht oder vernichtet werden. Administrations- und Supportzugriffe erfolgen nur im erforderlichen Umfang.

4. Kategorien betroffener Personen

Betroffen sein können insbesondere Kunden und Interessenten des Kunden, Website- und Landingpage-Besucher, Newsletter-Empfänger, Nutzer von Formularen, Chatbots, Terminbuchungs-, Telefonie-, CRM-, Funnel- und Automatisierungssystemen, Ansprechpartner bei Unternehmen, Beschäftigte, Bewerber, freie Mitarbeiter, Lieferanten, Dienstleister, Geschäftspartner und Teilnehmer digitaler Angebote.

5. Kategorien personenbezogener Daten

Verarbeitet werden können insbesondere Stamm- und Kontaktdaten, Unternehmens-, Berufs- und Funktionsdaten, Kommunikations- und Inhaltsdaten, Vertrags-, Kunden-, Interessenten-, Vertriebs- und Vorgangsdaten, Formular-, Termin-, Buchungs- und Kalenderdaten, Telefonie- und Gesprächsmetadaten, Newsletter- und Marketingdaten, Nutzungs-, Geräte-, Browser-, Cookie-, Tracking-, Log- und Zugriffsdaten, IP-Adressen, Support- und Fehlerdaten, Zugangsdaten, technische Identifikatoren sowie Medien- und Dokumentinhalte.

6. Besondere Kategorien personenbezogener Daten

Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO sowie Daten nach Art. 10 DSGVO sind grundsätzlich nicht Gegenstand der Leistungen. Ihre Verarbeitung setzt eine ausdrückliche projektbezogene Vereinbarung und zusätzliche angemessene Schutzmaßnahmen voraus.

7. Verarbeitungsorte

Die Verarbeitung erfolgt grundsätzlich in Deutschland, der Europäischen Union oder dem Europäischen Wirtschaftsraum. Soweit in Anlage 2 aufgeführte Dienstleister eine Verarbeitung in Drittländern vornehmen, gelten § 13 dieser AVV und die dort genannten Übermittlungsmechanismen.

8. Dauer der Verarbeitung und Löschung

Die Verarbeitung dauert für die Laufzeit der jeweiligen beauftragten Leistung. Nach Beendigung werden Daten nach Maßgabe von § 17 gelöscht oder zurückgegeben. Für Backups gelten die regulären Lösch- und Überschreibungszyklen; gesetzliche Aufbewahrungspflichten bleiben unberührt.

9. Verantwortungsabgrenzung

Der Kunde bleibt für die Rechtmäßigkeit der Verarbeitung, die Rechtsgrundlagen, Informationspflichten, Einwilligungen, Inhalte, Weisungen und die von ihm administrierten Nutzerkonten verantwortlich. WERTEweb ist für die weisungsgemäße Verarbeitung, die eigenen technischen und organisatorischen Maßnahmen und die ordnungsgemäße Einbindung eigener weiterer Auftragsverarbeiter verantwortlich.

10. Projektbezogene Konkretisierung

Soweit ein Projekt besondere Datenarten, erhöhte Risiken, abweichende Löschfristen, spezielle Sicherheitsanforderungen oder zusätzliche Dienstleister umfasst, werden diese Punkte im Angebot, Hauptvertrag, einer Leistungsbeschreibung oder einer dokumentierten Weisung konkretisiert. Eine gesonderte Unterschrift unter diese Anlage ist nicht erforderlich, wenn die AVV wirksam in das Vertragsverhältnis einbezogen wurde.

Stand und Aktualisierung

Stand: Juli 2026. Die WERTEweb GbR kann diese AVV und die Liste weiterer Auftragsverarbeiter im Rahmen der vertraglichen und gesetzlichen Vorgaben aktualisieren. Die jeweils aktuelle Fassung wird auf der Webseite der WERTEweb GbR bereitgestellt. Wesentliche Änderungen werden in geeigneter Weise mitgeteilt.