

Auftragsverarbeitungsvertrag

der Essential Advertising GmbH

Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag nach Artikel 28 der Verordnung (EU) 2016/679 (DSGVO)

Version 1.0 · gültig ab 10. August 2026

Abrufbar unter: <https://essentialadvertising.de/avv>

Wie dieser Vertrag zustande kommt

Dieser Auftragsverarbeitungsvertrag gilt für alle Kunden der Essential Advertising GmbH, bei deren Beauftragung personenbezogene Daten im Auftrag verarbeitet werden. Er wird mit Abschluss des Hauptvertrags automatisch wirksam. Eine gesonderte Unterschrift ist nicht erforderlich.

Art. 28 Abs. 9 DSGVO verlangt für den Auftragsverarbeitungsvertrag die Schriftform, lässt dafür aber ausdrücklich ein elektronisches Format zu. Die Einbeziehung dieses Dokuments in den Hauptvertrag erfüllt diese Anforderung.

Wer eine von beiden Seiten unterzeichnete Ausfertigung für die eigenen Unterlagen benötigt, fordert sie formlos unter mail@essentialadvertising.de an. Sie wird kostenfrei und in der Regel innerhalb von zwei Werktagen zur Verfügung gestellt. Am Inhalt ändert sich dadurch nichts.

Vertragsparteien

Auftragsverarbeiter

Essential Advertising GmbH
Adenauerallee 2
61440 Oberursel (Taunus)
Deutschland

Vertreten durch den Geschäftsführer Daniel Klantke
Handelsregister: Amtsgericht Bad Homburg v. d. Höhe, HRB 15288
USt-IdNr.: DE341132023
E-Mail: mail@essentialadvertising.de
Telefon: +49 6172 90 84 747

Nachfolgend „Auftragnehmer“.

Verantwortlicher

Der Kunde, der die Essential Advertising GmbH mit einer Leistung nach Anlage 1 beauftragt hat. Die Angaben zur Person des Verantwortlichen ergeben sich aus dem Hauptvertrag, dem angenommenen Angebot oder der Auftragsbestätigung.

Nachfolgend „Auftraggeber“.

§ 1 Geltung, Einbeziehung und Rangfolge

- (1) Dieser Vertrag ist Bestandteil jedes Vertrags zwischen dem Auftraggeber und dem Auftragnehmer, in dessen Rahmen der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers verarbeitet. Er wird ohne gesonderte Erklärung mit Abschluss des Hauptvertrags wirksam.
- (2) Als Hauptvertrag gilt jedes angenommene Angebot, jede Auftragsbestätigung sowie jeder Pflege-, Betreuungs- oder Hostingvertrag zwischen den Parteien.
- (3) Bei Widersprüchen zwischen diesem Vertrag, dem Hauptvertrag und den Allgemeinen Geschäftsbedingungen des Auftragnehmers gilt für alle Fragen des Datenschutzes ausschließlich dieser Vertrag.
- (4) Abweichende oder entgegenstehende Datenschutzbedingungen des Auftraggebers werden nicht Vertragsbestandteil, es sei denn, der Auftragnehmer stimmt ihnen in Textform ausdrücklich zu.
- (5) Die jeweils gültige Fassung dieses Vertrags ist unter <https://essentialadvertising.de/avv> abrufbar. Frühere Fassungen bleiben dort dauerhaft mit Versionsnummer und Gültigkeitszeitraum einsehbar, damit jederzeit nachvollziehbar ist, welche Fassung zu welchem Zeitpunkt galt.

§ 2 Gegenstand und Dauer

- (1) Gegenstand des Auftrags ist die Verarbeitung personenbezogener Daten, die zur Erbringung der im Hauptvertrag vereinbarten Leistungen erforderlich ist. Art und Zweck der Verarbeitung, die Kategorien personenbezogener Daten sowie die Kategorien betroffener Personen ergeben sich aus **Anlage 1**. Welche der dort beschriebenen Verarbeitungen im Einzelfall stattfinden, richtet sich nach dem im Hauptvertrag vereinbarten Leistungsumfang.
- (2) Die Laufzeit dieses Vertrags entspricht der Laufzeit des Hauptvertrags. Nach dessen Ende gelten die Pflichten aus § 11 fort.
- (3) Der Auftraggeber kann diesen Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen datenschutzrechtliche Vorschriften oder gegen die Pflichten aus diesem Vertrag vorliegt, wenn der Auftragnehmer eine Weisung nicht ausführen kann oder will oder wenn er Kontrollrechte vertragswidrig verweigert.

§ 3 Ort der Verarbeitung

- (1) Die Verarbeitung findet in Mitgliedstaaten der Europäischen Union oder in Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum statt. Die eingesetzten Rechenzentren befinden sich in Deutschland (Frankfurt am Main) und in Irland.

(2) Soweit einzelne der in **Anlage 3** genannten Unterauftragsverarbeiter ihren Sitz außerhalb der Europäischen Union haben oder von dort auf Verwaltungs- und Supportebene zugreifen können, erfolgt die Übermittlung ausschließlich auf Grundlage der in Anlage 3 genannten Garantien nach Art. 44 bis 49 DSGVO, insbesondere auf Grundlage von Standardvertragsklauseln der Europäischen Kommission oder eines Angemessenheitsbeschlusses.

§ 4 Weisungsrecht des Auftraggebers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers. Das gilt auch für die Übermittlung in ein Drittland. Eine Ausnahme besteht nur, wenn der Auftragnehmer nach dem Recht der Union oder eines Mitgliedstaats zur Verarbeitung verpflichtet ist. In diesem Fall teilt er dem Auftraggeber die rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Der Hauptvertrag und dieser Vertrag stellen die ursprüngliche Weisung des Auftraggebers dar. Weitere Weisungen erfolgen in Textform. E-Mail genügt. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich in Textform.

(3) Weisungsberechtigt sind die im Hauptvertrag benannten Ansprechpartner des Auftraggebers sowie Personen, die aus dem Verantwortungsbereich des Auftraggebers erkennbar berechtigt handeln. Weisungsempfänger auf Seiten des Auftragnehmers ist Daniel Klantke, mail@essentialadvertising.de.

(4) Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, weist er den Auftraggeber unverzüglich darauf hin. Er ist berechtigt, die Ausführung der betreffenden Weisung auszusetzen, bis der Auftraggeber sie bestätigt oder ändert.

(5) Der Auftragnehmer dokumentiert Weisungen sowie deren Umsetzung und bewahrt die Dokumentation für die Dauer des Vertrags sowie drei Jahre darüber hinaus auf.

§ 5 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet die Daten ausschließlich im Rahmen des Auftrags und der Weisungen. Eine Nutzung für eigene Zwecke findet nicht statt. Insbesondere werden Daten des Auftraggebers nicht zum Training von Modellen künstlicher Intelligenz verwendet. Der Auftragnehmer hat mit den in Anlage 3 genannten Anbietern künstlicher Intelligenz vertraglich sichergestellt, dass auch dort keine Nutzung zu Trainingszwecken erfolgt.

(2) Der Auftragnehmer verpflichtet alle Personen, die Zugang zu personenbezogenen Daten haben, schriftlich zur Vertraulichkeit, soweit sie nicht bereits einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Verpflichtung besteht auch nach Beendigung der Tätigkeit fort.

(3) Der Auftragnehmer führt ein Verzeichnis aller Kategorien von Verarbeitungstätigkeiten im Auftrag nach Art. 30 Abs. 2 DSGVO und stellt es dem Auftraggeber auf Anfrage zur Verfügung.

(4) Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung von dessen Pflichten nach Art. 32 bis 36 DSGVO, insbesondere bei der Sicherheit der Verarbeitung, bei der Meldung von Datenschutzverletzungen, bei der Benachrichtigung betroffener Personen sowie bei Datenschutz-Folgenabschätzungen und vorherigen

Konsultationen. Die Unterstützung erfolgt im Rahmen des Zumutbaren und unter Berücksichtigung der dem Auftragnehmer zur Verfügung stehenden Informationen.

(5) Der Auftragnehmer hat keinen Datenschutzbeauftragten bestellt, da die Voraussetzungen des Art. 37 DSGVO und des § 38 BDSG nicht vorliegen. Ansprechpartner für alle Fragen des Datenschutzes ist der Geschäftsführer Daniel Klantke, mail@essentialadvertising.de. Der Auftragnehmer teilt es mit, sobald ein Datenschutzbeauftragter bestellt wird.

(6) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn eine Aufsichtsbehörde beim Auftragnehmer Maßnahmen ergreift, die Verarbeitungen für den Auftraggeber betreffen könnten.

(7) Werden die Daten des Auftraggebers beim Auftragnehmer durch Pfändung, Beschlagnahme, Insolvenz- oder Vergleichsverfahren oder durch sonstige Maßnahmen Dritter gefährdet, informiert der Auftragnehmer den Auftraggeber unverzüglich.

§ 6 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer trifft die zur Sicherheit der Verarbeitung erforderlichen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO. Die getroffenen Maßnahmen sind in **Anlage 2** beschrieben. Der Auftraggeber erkennt sie mit Abschluss des Hauptvertrags als angemessen an.

(2) Die Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragnehmer darf sie anpassen, solange das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen dokumentiert er und macht sie in der jeweils gültigen Fassung dieses Vertrags einsehbar.

(3) Der Auftragnehmer überprüft die Wirksamkeit der Maßnahmen regelmäßig, mindestens jedoch einmal jährlich.

§ 7 Unterauftragsverhältnisse

(1) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine schriftliche Genehmigung nach Art. 28 Abs. 2 Satz 2 DSGVO, weitere Auftragsverarbeiter einzusetzen.

(2) Die genehmigten Unterauftragsverarbeiter sind in **Anlage 3** abschließend aufgeführt. Nicht jeder dieser Anbieter kommt bei jedem Auftrag zum Einsatz. Welche tatsächlich eingesetzt werden, richtet sich nach dem im Hauptvertrag vereinbarten Leistungsumfang. Anlage 3 weist dazu für jeden Anbieter aus, bei welcher Leistung er zum Einsatz kommt.

(3) Beabsichtigt der Auftragnehmer, einen weiteren Unterauftragsverarbeiter hinzuzuziehen oder einen bestehenden zu ersetzen, informiert er den Auftraggeber mindestens 30 Tage vorher in Textform an die zuletzt bekannte E-Mail-Adresse. Der Auftraggeber kann der Änderung innerhalb von 14 Tagen nach Zugang der Information aus wichtigem datenschutzrechtlichem Grund widersprechen. Widerspricht er, suchen die Parteien zunächst eine einvernehmliche Lösung. Kommt sie nicht zustande, sind beide Seiten berechtigt, den Hauptvertrag zum Zeitpunkt der geplanten Änderung zu kündigen.

(4) Der Auftragnehmer schließt mit jedem Unterauftragsverarbeiter einen Vertrag, der diesem dieselben Datenschutzpflichten auferlegt, die in diesem Vertrag festgelegt sind. Er wählt Unterauftragsverarbeiter sorgfältig aus und prüft vor Beauftragung sowie danach regelmäßig, ob sie die erforderlichen Garantien bieten.

(5) Kommt ein Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet der Auftragnehmer dem Auftraggeber gegenüber für dessen Verhalten wie für eigenes.

(6) Nicht als Unterauftragsverhältnis im Sinne dieser Regelung gelten Nebenleistungen, die der Auftragnehmer bei Dritten in Anspruch nimmt, etwa Telekommunikationsleistungen, Reinigung, Wartung durch Hersteller oder die Entsorgung von Datenträgern. Auch hier stellt der Auftragnehmer den Schutz der Daten sicher.

§ 8 Rechte betroffener Personen

(1) Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen dabei, Anträgen betroffener Personen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit und Widerspruch nachzukommen.

(2) Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, leitet dieser das Anliegen unverzüglich, spätestens innerhalb von drei Werktagen, an den Auftraggeber weiter. Der Auftragnehmer beantwortet solche Anfragen nicht selbst, es sei denn, der Auftraggeber weist ihn dazu an.

(3) Berichtigung, Löschung und Einschränkung von Daten nimmt der Auftragnehmer nur auf Weisung des Auftraggebers vor.

§ 9 Nachweise und Kontrollen

(1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der Pflichten aus diesem Vertrag auf Anfrage nach, insbesondere durch die Dokumentation der technischen und organisatorischen Maßnahmen nach Anlage 2 sowie durch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Stellen und durch geeignete Zertifizierungen der eingesetzten Unterauftragsverarbeiter.

(2) Der Auftraggeber ist berechtigt, sich von der Einhaltung dieses Vertrags durch Überprüfungen zu überzeugen, auch durch Inspektionen vor Ort. Er kündigt Kontrollen mit angemessener Frist, in der Regel 14 Tagen, an und führt sie zu üblichen Geschäftszeiten sowie ohne vermeidbare Störung des Betriebsablaufs durch. Der Auftragnehmer wirkt an den Kontrollen mit.

(3) Der Auftraggeber trägt die Kosten seiner Kontrollen. Für den Aufwand des Auftragnehmers ab der zweiten Kontrolle innerhalb eines Kalenderjahres kann dieser eine angemessene Vergütung verlangen, sofern kein konkreter Anlass für die weitere Kontrolle besteht.

(4) Der Auftraggeber darf Kontrollen durch beauftragte Dritte durchführen lassen. Der Auftragnehmer kann Dritten widersprechen, die zu ihm in einem Wettbewerbsverhältnis stehen.

§ 10 Meldung von Verletzungen des Schutzes personenbezogener Daten

(1) Der Auftragnehmer meldet dem Auftraggeber jede Verletzung des Schutzes personenbezogener Daten unverzüglich nach Bekanntwerden, spätestens innerhalb von 24 Stunden. Dasselbe gilt bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verstöße gegen Datenschutzvorschriften sowie bei Verdacht auf Verstöße gegen diesen Vertrag.

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

(3) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen. Er stimmt sich dabei mit dem Auftraggeber ab.

(4) Meldungen an die Aufsichtsbehörde nach Art. 33 DSGVO sowie Benachrichtigungen betroffener Personen nach Art. 34 DSGVO nimmt ausschließlich der Auftraggeber vor.

§ 11 Löschung und Rückgabe nach Beendigung

(1) Nach Abschluss der Erbringung der Verarbeitungsleistungen löscht der Auftragnehmer alle personenbezogenen Daten oder gibt sie zurück. Der Auftraggeber wählt zwischen Löschung und Rückgabe und teilt seine Wahl spätestens bei Vertragsende in Textform mit. Ohne Mitteilung erfolgt die Löschung.

(2) Die Löschung erfolgt innerhalb von 60 Tagen nach Vertragsende. Sie umfasst auch Kopien bei Unterauftragsverarbeitern. Der Auftragnehmer weist die Löschung auf Anfrage in Textform nach.

(3) Von der Löschung ausgenommen sind Daten, für die eine gesetzliche Aufbewahrungspflicht besteht, insbesondere nach § 147 AO und § 257 HGB. Diese Daten werden für die Dauer der Aufbewahrungsfrist gesperrt und danach gelöscht.

(4) Sicherungskopien in Backups werden nach dem regulären Sicherungszyklus überschrieben. Ein vorzeitiges Löschen einzelner Datensätze aus Sicherungskopien ist technisch nicht möglich. Bis zum Überschreiben bleiben diese Daten gesperrt.

(5) Ergebnisse der Leistung, an denen der Auftraggeber Rechte erworben hat, insbesondere Websites, Gestaltungsdateien und Bildmaterial, bleiben von diesem Paragraphen unberührt und werden nach den Regeln des Hauptvertrags übergeben.

§ 12 Pflichten des Auftraggebers

(1) Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Rechte betroffener Personen allein verantwortlich.

(2) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er bei der Prüfung der Ergebnisse Fehler oder Unregelmäßigkeiten in Bezug auf datenschutzrechtliche Vorschriften feststellt.

(3) Der Auftraggeber stellt sicher, dass für Fotografien, auf denen Personen erkennbar sind, die erforderlichen Einwilligungen oder sonstigen Rechtsgrundlagen vorliegen, bevor er entsprechendes Material übergibt oder ein Shooting beauftragt. Der Auftragnehmer stellt hierfür auf Wunsch eine Vorlage zur Verfügung.

(4) Überträgt der Auftraggeber dem Auftragnehmer Empfänger- oder Kontaktlisten für den Versand von Nachrichten, gewährleistet er, dass für jeden Empfänger eine wirksame Rechtsgrundlage vorliegt und dass er diese nachweisen kann.

(5) Der Auftraggeber übermittelt dem Auftragnehmer keine Daten besonderer Kategorien nach Art. 9 DSGVO, soweit dies nicht ausdrücklich vereinbart ist.

§ 13 Haftung

- (1) Für die Haftung gelten Art. 82 DSGVO sowie die Regelungen des Hauptvertrags.
- (2) Der Auftragnehmer haftet gegenüber dem Auftraggeber nicht, soweit ein Schaden auf einer Weisung des Auftraggebers beruht, auf deren Rechtswidrigkeit der Auftragnehmer nach § 4 Abs. 4 hingewiesen hat.

§ 14 Änderungen dieses Vertrags

- (1) Der Auftragnehmer darf diesen Vertrag ändern, wenn dies aufgrund geänderter Rechtslage, geänderter Rechtsprechung, behördlicher Vorgaben oder wesentlicher Änderungen der eingesetzten Technik erforderlich ist. Änderungen dürfen das Schutzniveau für den Auftraggeber und die betroffenen Personen nicht verringern.
- (2) Der Auftragnehmer kündigt Änderungen mindestens 30 Tage vor Inkrafttreten in Textform an die zuletzt bekannte E-Mail-Adresse an und veröffentlicht die neue Fassung unter <https://essentialadvertising.de/avv>.
- (3) Der Auftraggeber kann der Änderung innerhalb von 30 Tagen nach Zugang der Ankündigung in Textform widersprechen. Widerspricht er, gilt die bisherige Fassung fort. Ist dem Auftragnehmer die Fortführung zu den bisherigen Bedingungen nicht zumutbar, kann er den Hauptvertrag mit einer Frist von einem Monat kündigen.
- (4) Änderungen von **Anlage 3** richten sich ausschließlich nach § 7 Abs. 3.

§ 15 Schlussbestimmungen

- (1) Änderungen und Ergänzungen bedürfen der Textform. Das gilt auch für die Aufhebung dieser Formklausel. § 14 bleibt unberührt.
- (2) Sollte eine Bestimmung dieses Vertrags 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.
- (3) Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts.
- (4) Ist der Auftraggeber Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen, ist Gerichtsstand der Sitz des Auftragnehmers.
-

Unterschriften

Dieser Vertrag wird nach § 1 Abs. 1 ohne Unterschrift wirksam. Die folgenden Felder dienen ausschließlich dem Fall, dass der Auftraggeber eine unterzeichnete Ausfertigung für seine Unterlagen wünscht. Sie sind für die Wirksamkeit ohne Bedeutung.

Auftraggeber

Firma: _____

Ort, Datum: _____

Unterschrift, Name in Druckbuchstaben: _____

Auftragnehmer, Essential Advertising GmbH

Ort, Datum: Oberursel (Taunus), _____

Unterschrift: _____

Daniel Klantke, Geschäftsführer

Anlage 1: Beschreibung der Verarbeitung

Diese Anlage beschreibt sämtliche Verarbeitungen, die im Rahmen des Leistungsangebots der Essential Advertising GmbH vorkommen können. Maßgeblich ist im Einzelfall der im Hauptvertrag vereinbarte Leistungsumfang. Verarbeitungen, die zu einer nicht beauftragten Leistung gehören, finden nicht statt.

1. Gegenstand und Art der Verarbeitung

Der Auftragnehmer erbringt für den Auftraggeber Leistungen aus den folgenden Bereichen:

Webdesign und Webentwicklung. Konzeption, Gestaltung, technische Umsetzung und Inbetriebnahme von Websites, Onepagern und Landingpages einschließlich Formularen, Buchungstrecken und Auswertungen.

Betrieb, Hosting und Pflege. Bereitstellung der Website auf der Infrastruktur des Auftragnehmers, Wartung, Sicherheitsaktualisierungen, Sicherungskopien, Störungsbeseitigung sowie redaktionelle Pflege von Inhalten.

Kundenportal. Bereitstellung des Portals unter portal.essentialadvertising.de zur Projektabwicklung mit Zugängen, Freigaben, Anmerkungen, Terminen, Dokumenten und Rechnungen.

Fotografie. Aufnahme, Bearbeitung, Speicherung, Freigabe und Auslieferung von Bildmaterial über Galerien und Übertragungslinks.

Social Media. Erstellung, Planung und Veröffentlichung von Beiträgen sowie Bearbeitung eingehender Nachrichten und Kommentare in den vom Auftraggeber freigegebenen Kanälen.

Reichweitenmessung. Cookiefreie Auswertung der Websitenutzung ohne Speicherung von IP-Adressen.

Newsletter und E-Mail-Marketing. Bereitstellung des Produkts bemailed. Hierfür gilt ergänzend und vorrangig der eigene Auftragsverarbeitungsvertrag unter <https://www.bemailed.de/newsletter-tool/legal/avv>.

Angebots-, Freigabe- und Feedbackstrecken. Bereitstellung von Links zur Angebotsannahme, zur Bildauswahl und zur Rückmeldung zu Websiteentwürfen, jeweils ohne Konto und mit zeitlicher Befristung.

Die Verarbeitung erfolgt überwiegend automatisiert, in Teilen manuell.

2. Zweck der Verarbeitung

Die Verarbeitung dient ausschließlich der Erbringung der beauftragten Leistungen, insbesondere dem technischen Betrieb, der Fehlersuche, der Sicherstellung der Datensicherheit, der Kommunikation mit dem Auftraggeber und mit dessen Kunden im Rahmen der beauftragten Kanäle sowie der Bereitstellung der vereinbarten Auswertungen. Eine Verarbeitung zu eigenen Zwecken des Auftragnehmers findet nicht statt.

3. Kategorien betroffener Personen

Je nach beauftragter Leistung können betroffen sein:

- Beschäftigte des Auftraggebers
- Kunden und Interessenten des Auftraggebers
- Besucher der Website des Auftraggebers
- Empfänger von Newslettern und sonstigen Nachrichten des Auftraggebers
- Auf Fotografien abgebildete Personen
- Ansprechpartner bei Lieferanten und Geschäftspartnern des Auftraggebers

4. Kategorien personenbezogener Daten

Je nach beauftragter Leistung können verarbeitet werden:

Kategorie	Beispiele
Stammdaten	Name, Anrede, Funktion, Firma
Kontaktdaten	E-Mail-Adresse, Telefonnummer, Postanschrift
Vertrags- und Abrechnungsdaten	Auftragsdaten, Rechnungen, Zahlungsstatus
Inhaltsdaten	Nachrichten aus Formularen, Kommentare, Anmerkungen, hochgeladene Dateien
Nutzungsdaten	Aufgerufene Seiten, verweisende Seite, Zeitpunkt, Gerätetyp, Browser, Betriebssystem
Verbindungsdaten	IP-Adresse in Server-Protokollen
Zugangsdaten	Benutzerkonten, Passwort-Prüfwerte, Anmeldezeitpunkte, Sitzungskennungen
Bildmaterial	Fotografien, auf denen Personen erkennbar sind

Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO sind nicht Gegenstand des Auftrags. Werden sie ausnahmsweise übermittelt, etwa durch Angaben in freien Textfeldern, verarbeitet der Auftragnehmer sie ausschließlich zur Weiterleitung an den Auftraggeber und löscht sie danach unverzüglich.

5. Dauer der Verarbeitung und Löschfristen

Die Verarbeitung erfolgt für die Dauer des Hauptvertrags. Anschließend gilt § 11. Innerhalb der Laufzeit gelten folgende Fristen:

Datenart	Aufbewahrung
Server-Protokolle mit IP-Adresse	maximal 30 Tage
Nutzungsdaten der Reichweitenmessung	14 Monate, ohne Personenbezug
Nachrichten aus Formularen	bis zur Erledigung, danach maximal 6 Monate
Links zu Angeboten, Galerien, Übertragungen und Feedback	bis zum Ablaufdatum des jeweiligen Links
Projekt- und Auftragsdaten im Kundenportal	Dauer der Geschäftsbeziehung
Bildmaterial	Dauer der Geschäftsbeziehung, danach Übergabe oder Löschung
Rechnungsdaten	10 Jahre nach § 147 AO

Anlage 2: Technische und organisatorische Maßnahmen

nach Art. 32 DSGVO · Stand 10. August 2026

1. Vertraulichkeit

1.1 Zutrittskontrolle

Der Auftragnehmer betreibt keine eigenen Server. Die gesamte Datenverarbeitung findet in zertifizierten Rechenzentren der in Anlage 3 genannten Anbieter statt. Diese verfügen über Zutrittskontrollen mit Vereinzelungsanlagen, Videoüberwachung, Besucherprotokollierung sowie eine ständige Besetzung. Nachweise liegen in Form von ISO-27001- und SOC-2-Berichten der Anbieter vor.

Die Geschäftsräume des Auftragnehmers sind außerhalb der Arbeitszeiten verschlossen. Ein Zugang für Dritte besteht nur in Begleitung.

1.2 Zugangskontrolle

- Alle Arbeitsgeräte sind mit Festplattenverschlüsselung gesichert.
- Der Zugang zu Geräten erfolgt über Kennwort oder biometrische Merkmale, mit automatischer Sperre nach Inaktivität.
- Für alle Dienste, die personenbezogene Daten verarbeiten, ist Zwei-Faktor-Authentifizierung aktiviert.
- Kennwörter werden ausschließlich in einem Kennwortverwaltungsprogramm gespeichert, niemals in Dateien, Chatverläufen oder im Quellcode.

- Zugangsdaten und Schlüssel für Produktivsysteme liegen ausschließlich in der verschlüsselten Umgebungsvariablen-Verwaltung des Hosting-Anbieters.
- Benutzerkonten in den bereitgestellten Anwendungen werden über einen spezialisierten Authentifizierungsdienst verwaltet. Kennwörter werden ausschließlich als Prüfwert gespeichert.
- Anmeldeversuche sind mengenmäßig begrenzt, um automatisierte Angriffe zu verhindern.

1.3 Zugriffskontrolle

- Der Zugriff auf Daten folgt dem Grundsatz der geringsten Rechte. Jede Person erhält nur die Rechte, die für ihre Aufgabe erforderlich sind.
- In der Datenbank ist eine zeilenbasierte Zugriffskontrolle (Row Level Security) durchgängig aktiviert. Sie stellt sicher, dass jedes Konto ausschließlich die eigenen Datensätze lesen und schreiben kann. Der Schutz wirkt auf Datenbankebene, unabhängig von der Anwendung.
- Privilegierte Datenfelder wie Rollen oder Guthaben sind zusätzlich durch Datenbank-Auslöser gegen Veränderung durch Nutzerkonten gesichert.
- Dateien liegen in privaten Speicherbereichen und werden ausschließlich über zeitlich befristete, signierte Verweise ausgeliefert.
- Administrative Zugriffe erfolgen ausschließlich über gesonderte, serverseitig geprüfte Berechtigungen.
- Ein Vorschau-Modus für administrative Konten ist schreibgeschützt.

1.4 Trennungskontrolle

- Daten unterschiedlicher Auftraggeber werden logisch getrennt und über Mandantenkennungen sowie die zeilenbasierte Zugriffskontrolle voneinander abgesichert.
- Test-, Entwicklungs- und Produktivumgebungen sind getrennt. In Entwicklungsumgebungen werden keine echten personenbezogenen Daten verwendet.

1.5 Pseudonymisierung und Datenminimierung

- Die Reichweitenmessung speichert keine IP-Adressen. Die IP-Adresse fließt lediglich in einen täglich wechselnden, nicht umkehrbaren Prüfwert ein, der ausschließlich der Zusammenfassung von Seitenaufrufen eines Tages dient. Eine geräteübergreifende Wiedererkennung ist damit technisch ausgeschlossen.
- Es werden keine Cookies zu Analyse- oder Marketingzwecken gesetzt, solange keine Einwilligung vorliegt.
- Formulare erheben nur die Felder, die für den jeweiligen Zweck erforderlich sind.

2. Integrität

2.1 Weitergabekontrolle

- Sämtliche Datenübertragungen erfolgen ausschließlich verschlüsselt über TLS in aktueller Version. Unverschlüsselte Zugriffe werden umgeleitet.
- Es besteht ein durchgängiger Transportsicherheits-Header (HSTS).
- Der E-Mail-Versand erfolgt über authentifizierte Verbindungen mit SPF, DKIM und DMARC.
- Datenträger werden nicht versendet. Der Austausch von Dateien erfolgt über die bereitgestellten Portale mit zeitlich befristeten Verweisen.

- Ausgemusterte Datenträger werden vor der Entsorgung sicher gelöscht.

2.2 Eingabekontrolle

- Änderungen an Projekt-, Auftrags- und Abrechnungsdaten werden mit Zeitstempel und auslösendem Konto protokolliert.
- Administrative Vorgänge sind in einem Protokoll nachvollziehbar.
- Der gesamte Quellcode wird versioniert. Jede Änderung ist einer Person und einem Zeitpunkt zuordenbar.

3. Verfügbarkeit und Belastbarkeit

- Die eingesetzte Infrastruktur ist mehrfach redundant ausgelegt und über mehrere Verfügbarkeitszonen verteilt.
- Von der Datenbank werden tägliche automatische Sicherungen erstellt. Zusätzlich besteht eine zeitpunktgenaue Wiederherstellung über einen Zeitraum von sieben Tagen.
- Sicherungen liegen verschlüsselt und innerhalb der EU.
- Die Wiederherstellbarkeit wird mindestens einmal jährlich überprüft.
- Der Betrieb wird laufend überwacht. Fehler in Produkktivsystemen lösen eine automatische Benachrichtigung aus.
- Abhängigkeiten werden regelmäßig auf bekannte Schwachstellen geprüft und aktualisiert.
- Schutz gegen Überlastung und automatisierte Angriffe besteht auf Ebene des Content-Delivery-Netzwerks sowie durch Begrenzung der Anfragehäufigkeit an sensiblen Endpunkten.

4. Verfahren zur Überprüfung und Bewertung

4.1 Datenschutz-Management

- Der Geschäftsführer ist zuständig für alle Fragen des Datenschutzes.
- Ein Verzeichnis der Verarbeitungstätigkeiten wird geführt und mindestens jährlich überprüft.
- Alle Personen mit Zugang zu personenbezogenen Daten sind schriftlich zur Vertraulichkeit verpflichtet.
- Mit allen Dienstleistern, die personenbezogene Daten im Auftrag verarbeiten, bestehen Verträge nach Art. 28 DSGVO.

4.2 Vorfall-Management

- Für Verletzungen des Schutzes personenbezogener Daten besteht ein festgelegter Ablauf mit Meldung an den Auftraggeber innerhalb von 24 Stunden.
- Vorfälle werden dokumentiert und ausgewertet.

4.3 Überprüfung

- Die technischen und organisatorischen Maßnahmen werden mindestens jährlich überprüft.
- Die Anwendungen werden regelmäßig auf Sicherheitslücken untersucht, unter anderem auf fehlerhafte Zugriffsregeln, unsichere Endpunkte und Rechteausweitung.

- Automatisierte Tests laufen bei jeder Änderung am Quellcode.

4.4 Datenschutz durch Technikgestaltung und Voreinstellungen

- Neue Datenbanktabellen erhalten standardmäßig eine sperrende Zugriffsregel. Der Zugriff wird anschließend gezielt freigegeben.
 - Öffentliche Freigabelinks laufen automatisch ab.
 - Es werden ausschließlich technisch notwendige Cookies gesetzt, solange keine Einwilligung vorliegt.
 - Nicht öffentliche Bereiche sind für Suchmaschinen gesperrt.
-

Anlage 3: Genehmigte Unterauftragsverarbeiter

Version 1.0 · Stand 10. August 2026

Die folgenden Unternehmen sind nach § 7 dieses Vertrags allgemein genehmigt. Nicht jeder Anbieter kommt bei jedem Auftrag zum Einsatz. Die Spalte „Eingesetzt bei“ weist aus, an welche Leistung der jeweilige Einsatz gebunden ist.

Unternehmen und Sitz	Leistung	Eingesetzt bei	Ort der Verarbeitung	Garantie für Drittlandbezug
Vercel Inc. , 340 S Lemon Ave #4133, Walnut, CA 91789, USA	Hosting der Web-Anwendung, Content-Delivery-Netzwerk	allen Leistungen	EU, Frankfurt am Main	Standardvertragsklauseln im DPA, EU-US Data Privacy Framework
Supabase Inc. , 970 Toa Payoh North #07-04, Singapur	Datenbank, Anmeldung, Dateispeicher	allen Leistungen	EU, Frankfurt am Main (eu-central-1)	Standardvertragsklauseln im DPA
Plus Five Five, Inc. (Resend) , 2261 Market Street #5039, San Francisco, CA 94114, USA	Versand von System- und Benachrichtigungs-E-Mails	allen Leistungen	USA, Zustellung weltweit	Standardvertragsklauseln im DPA, EU-US Data Privacy Framework
IONOS SE , Elgendorfer Straße 57, 56410 Montabaur, Deutschland	Domains, DNS	Website, Hosting	Deutschland	kein Drittlandbezug
Microsoft Ireland Operations Ltd. , One Microsoft Place, Dublin 18, Irland	Geschäfts-E-Mail und Bürosoftware	allen Leistungen	EU	Standardvertragsklauseln im Microsoft DPA
Functional Software, Inc. (Sentry) , 45 Fremont Street, San Francisco, CA 94105, USA	Erfassung technischer Fehlermeldungen	Website, Hosting, Portal	EU-Region	Standardvertragsklauseln im DPA
Stripe Payments Europe Ltd. , 1 Grand Canal Street Lower,	Zahlungsabwicklung	Online-Zahlung	EU, teilweise USA	Standardvertragsklauseln im Stripe DPA

Unternehmen und Sitz	Leistung	Eingesetzt bei	Ort der Verarbeitung	Garantie für Drittlandbezug
Dublin 2, Irland				
Cal.com, Inc. (EU-Instanz cal.eu)	Online-Terminbuchung	Portal, Terminbuchung	EU, Irland	Standardvertragsklauseln
Anthropic PBC , 548 Market St, San Francisco, CA 94104, USA	Textvorschläge und Auswertungen mit künstlicher Intelligenz	KI-gestützten Funktionen	USA	Standardvertragsklauseln im DPA, EU-US Data Privacy Framework
OpenAI Ireland Ltd. , 1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, Irland	Textvorschläge mit künstlicher Intelligenz	KI-gestützten Funktionen	EU, teilweise USA	Standardvertragsklauseln im DPA
Google Ireland Ltd. , Gordon House, Barrow Street, Dublin 4, Irland	Kartendaten, Unternehmensangaben, Werbe-Erfolgsmessung nur mit Einwilligung	Website, Kampagnen	EU, teilweise USA	Google Ads Datenverarbeitungsbedingungen, Standardvertragsklauseln
Amazon Web Services EMEA SARL , 38 Avenue John F. Kennedy, L-1855 Luxemburg	Massenversand von E-Mails	Newsletter über bemailed	EU, Frankfurt am Main	AWS GDPR DPA, Bestandteil der Service Terms
Upstash, Inc. , 1606 Headway Cir #9531, Austin, TX 78754, USA	Begrenzung der Anfragehäufigkeit, Zwischenspeicher	Newsletter über bemailed	EU	Standardvertragsklauseln im DPA
Inngest, Inc. , 2261 Market	zeitgesteuerte Hintergrundaufgaben	Newsletter über bemailed	USA	Standardvertragsklauseln im DPA

Unternehmen und Sitz	Leistung	Eingesetzt bei	Ort der Verarbeitung	Garantie für Drittlandbezug
Street #5309, San Francisco, CA 94114, USA				

Bei den Anbietern künstlicher Intelligenz ist vertraglich sichergestellt, dass Daten des Auftraggebers nicht zum Training von Modellen verwendet werden.

Änderungen dieser Anlage werden nach § 7 Abs. 3 angekündigt. Die jeweils gültige Fassung mit Versionsnummer steht unter <https://essentialadvertising.de/avv>.

Version 1.0, gültig ab 10. August 2026. Erstellt nach Art. 28 DSGVO und auf die tatsächlichen Verarbeitungen der Essential Advertising GmbH zugeschnitten. Ersetzt keine anwaltliche Prüfung des Einzelfalls.