Vereinbarung zur Auftragsverarbeitung gem. Art. 28 EU-DS-GVO

zwischen

Kunde

Strasse Nr.

PLZ Ort

vertreten durch

Name

Position

Verantwortlicher, nachstehend Auftraggeber genannt

und

Medien-Service Untermain GmbH

Weichertstraße 20

D-63741 Aschaffenburg

vertreten durch

Herrn Ulrich Eymann

(Geschäftsführer)

Auftragsverarbeiter, nachstehend Auftragnehmer genannt

wird folgender Vertrag über Auftragsverarbeitung nach Art. 28 Abs. 3 und den weiteren Bestimmungen der Verordnung 2016/79 EU (EU Datenschutz-Grundverordnung) [i.F.: „EU-DS-GVO"], sowie sonstiger anwendbarer datenschutzrechtlicher Bestimmungen geschlossen:

§ 1 Gegenstand und Dauer des Auftrags, Auftragsinhalt

1. Inhalt

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers.
Inhalt des Vertrages ist die Regelung aller datenschutzrechtlicher Fragen zwischen Auftraggeber und Auftragnehmer.

2. Gegenstand des Auftrags

Der Gegenstand des Auftrags ergibt sich aus der dem Auftrag zugrundeliegenden Leistungsvereinbarung / SLA, auf die hier verwiesen wird (im Folgenden „Leistungsvereinbarung“).

3. Dauer des Auftrags

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

4. Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber:

- Erbringung von Dienstleistungen in Zusammenhang mit einem Produkt (Hard-/Software, Hostingleistung) des Auftragnehmers gemäß dem Hauptvertrag oder einer im jeweiligen Einzelfall erfolgten Beauftragung.

Die Leistungen sind konkret beschrieben in der Leistungsvereinbarung

5. Ort der Datenverarbeitung

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Information des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. EU-DS-GVO erfüllt sind.

6. Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten / -kategorien:

- Personenstammdaten
- Kommunikationsdaten (z. B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Auskunftsangaben (von Dritten, z. B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- Bei Hostingleistungen vom Kunden auf den bereitgestellten Systemen abgelegte Datenarten / –kategorien
- Nutzungs- und Protokolldaten (Verbrauch, Zugriffe)

- Ggfs. weitere / abweichende, im Hauptvertrag spezifizierte Datenarten / –kategorien

7. Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden
- Interessenten
- Beschäftigte
- Lieferanten / Handelspartner
- Ansprechpartner
- Ggfs. weitere / abweichende, im Hauptvertrag spezifizierte Kategorien betroffener Personen

§ 2 Pflichten / Kontrollrecht des Auftraggebers

1. Der Auftraggeber ist alleine verantwortlich für die Beurteilung der rechtlichen Zulässigkeit der im Rahmen des Auftragsverhältnisses durchzuführenden Verarbeitung durch den Auftragnehmer im Hinblick auf die Regelungen der EU Datenschutz-Grundverordnung und anderer Vorschriften über den Datenschutz.

2. Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 EU-DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann z.B. auch erfolgen durch:

- Die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 EU-DS-GVO
- Die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 EU-DS-GVO
- Aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren)
- Eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz, ISO 27001).

Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

Die Verarbeitung von Daten in Privatwohnungen ist gestattet. Auch dort werden die datenschutzrechtlichen Vorschriften eingehalten.

3. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

§ 3 Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 EU-DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

1. Schriftliche Bestellung eines Datenschutzbeauftragten, soweit gesetzlich erforderlich.

   Der bestellte Datenschutzbeauftragte beim Auftragnehmer ist der Anlage 3 zu entnehmen. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

2. Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 EU-DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Diese gelten auch nach Beendigung des Auftrags fort. Er verpflichtet sich, auch folgende relevanten Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen, sofern Sie für diesen Auftrag relevant sind:

   - Fernmeldegeheimnis
     (z.B. Bankgeheimnis, Fernmeldegeheimnis, Sozialgeheimnis, Berufsgeheimnisse §203 StGB etc.)

3. Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 EU-DS-GVO (Einzelheiten s. Anlage 1).

4. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

5. Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird.

6. Der Auftragnehmer verarbeitet personenbezogene Daten des Auftraggebers ausschließlich im Rahmen der vertraglich festgelegten Weisungen und der speziellen Einzelweisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedsstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist (beispielsweise bei Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden). In einem solchen Fall teilt der Auftragnehmer dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Er verwendet die zur Datenverarbeitung überlassenen Daten nicht für andere Zwecke und bewahrt sie nicht länger auf, als es der Auftraggeber bestimmt.

Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen Datenschutzvorschriften verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Weisungsberechtigten beim Auftraggeber bestätigt oder geändert wird.

7. Der Auftragnehmer ist verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Unterlagen und Daten betroffen sind. Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, wenn ein Datenschutz-Vorfall in Bezug auf den Vertragsgegenstand bekannt wird.

8. Der Auftragnehmer führt das Verzeichnis der Verarbeitungstätigkeit gem. Art. 30 Abs. 2 EU-DS-GVO und stellt dies auf Anfrage dem Auftraggeber zur Verfügung. Der Auftraggeber stellt dem Auftragnehmer die hierzu erforderlichen Informationen zur Verfügung. Der Auftragnehmer unterstützt den Auftraggeber seinerseits bei der Erstellung des Verzeichnisses nach Art 30 Abs. 1 EU-DS-GVO.

9. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der EU-DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten.

10. Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

11. Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

    Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

    Etwaig anfallende Mehrkosten für den Auftragnehmer im Rahmen dieser Pflichten sind diesem durch den Auftraggeber zu ersetzen.

§ 4 Rückgabe und Löschung

Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Kopien, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungsfristen erforderlich sind.

Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

§ 5 Unterauftragsverhältnisse

1. Der Auftragnehmer darf Unterauftragsverarbeiter (weitere Auftragsverarbeiter) nur nach vorheriger Zustimmung des Auftraggebers beauftragen.
   Der Auftraggeber stimmt der Beauftragung der in Anlage 2 aufgeführten Unterauftragsverarbeiter zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2 bis 4, 9 EU-DS-GVO, welche sowohl schriftlich als auch in einem elektronischen Format erfolgen kann.

2. Vor Hinzuziehung weiterer oder Ersetzung aufgeführter Unterauftragsverarbeiter informiert der Auftragnehmer den Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform.

3. Der Auftraggeber kann gegen die Änderung – innerhalb einer angemessenen Frist, jedoch nicht länger als 2 Wochen – aus wichtigem datenschutzrechtlichem Grund – gegenüber der vom Auftragnehmer bezeichneten Stelle Einspruch erheben. Erfolgt kein Einspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben. Bei unberechtigtem Einspruch kann es zu entsprechenden Verzögerungen bei der Erbringung der Leistung nach dem Hauptvertrag kommen. Für eine aus einem unberechtigten Einspruch resultierende Einschränkung der Vertragsleistungen ist der Auftragnehmer nicht verantwortlich.
   Hat der Auftraggeber aufgrund eines wichtigen datenschutzrechtlichen Grundes berechtigt Einspruch gegen einen Unterauftragsverarbeiter erhoben und ist eine einvernehmliche Lösungsfindung zwischen den Parteien auch auf anderem Wege aufgrund von wichtigen datenschutzrechtlichen Gründen nicht möglich, wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt. Ein wichtiger Grund liegt vor, wenn gegen wesentliche Bestimmungen dieses Vertrages verstoßen wurde oder wird.
   In Ausnahmefällen ist auch eine nachträgliche Einigung zwischen den Parteien möglich. Der Auftragnehmer hat den Auftraggeber in diesem Fall unverzüglich über den Einsatz eines Unterauftragsverarbeiters zu informieren.

4. Erbringt der Unterauftragsverarbeiter die vereinbarte Leistung außerhalb der EU / des EWR, stellen Auftraggeber und Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. In einem solchen Fall erfolgt eine Benachrichtigung des Auftraggebers.

5. Eine weitere Auslagerung durch den Unterauftragsverarbeiter bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mindestens Textform); sämtliche vertragliche Regelungen zu den Datenschutzpflichten in der Vertragskette sind auch dem weiteren Unterauftragsverarbeiter aufzuerlegen.

6. Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

§ 6 Weisungsrechte

Die Verarbeitung der Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers. Der Auftraggeber erteilt alle Weisungen und Aufträge in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und in schriftlicher oder elektronischer Form zu dokumentieren.

Mündliche Weisungen bestätigt der Auftraggeber unverzüglich schriftlich oder in einem dokumentierten elektronischen Format.

- Weisungsberechtigte Personen des Auftraggebers sind:

  Person 1

  Person 2

  Person 3

- Weisungsempfänger beim Auftragnehmer sind:
  Ulrich Eymann (Geschäftsführer),
  Michael Weis (Prokurist), Harald Salg (Prokurist)

Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners ist dem Vertragspartner unverzüglich schriftlich der Nachfolger bzw. der Vertreter mitzuteilen.

Weisungen des Auftraggebers an den Auftragnehmer werden ausschließlich von den o. g. verantwortlichen Sachgebietsbearbeitern erteilt.

§ 7 Rechte betroffener Personen

1. Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Der Auftragnehmer unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte betroffener Personen nach Art. 12 bis 22 EU-DS-GVO. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

2. Etwaige dem Auftragnehmer hierdurch entstehende Mehrkosten sind diesem durch den Auftraggeber zu erstatten.

§ 8 Haftung und Verantwortlichkeiten

Die vertragliche Haftung wird im Leistungsvertrag beschrieben. Auf diesen Vertrag wird im Rahmen der Auftragsverarbeitung verwiesen.

Unbeschadet der Artikel 82-84 EU-DS-GVO gilt ein Auftragsverarbeiter, der unter Verstoß gegen die datenschutzrechtlichen Bestimmungen die Zwecke und Mittel der Datenverarbeitung bestimmt, in Bezug auf diese Verarbeitung als Verantwortlicher.

Der Auftragsverarbeiter verpflichtet sich, angemessene und dem Stand der Technik entsprechende technische und organisatorische Maßnahmen umzusetzen. Die Einzelheiten werden im folgenden Kapitel (Kapitel 9) näher beschrieben. Die tatsächlich umgesetzten Maßnahmen werden im Anhang aufgelistet.

Der Verantwortliche (Auftraggeber) ist dazu berechtigt, die im Vertrag beschriebenen technischen und organisatorischen Maßnahmen regelmäßig zu überprüfen (Audit). Die Kostentragung wird im Leistungsvertrag definiert. Der Auftragsverarbeiter (Auftragnehmer) muss die Durchführung von Audits unterstützen. Der Verantwortliche erhält in diesem Zusammenhang Zugriff auf alle, für den jeweiligen Vertrag relevanten, Daten und Räumlichkeiten.

Legt der Auftragsverarbeiter (Auftragnehmer) ein Zertifikat nach den Anforderungen der Art. 40 ff. EU-DS-GVO vor, werden Audits nur bei einem konkreten Anlass durchgeführt.

§ 9 Technisch-organisatorische Maßnahmen

1. Die in der Anlage 1 beschriebenen technischen und organisatorischen Maßnahmen werden als verbindlich festgelegt.

   Der Auftragnehmer hat damit die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 EU-DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 EU-DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 EU-DS-GVO zu berücksichtigen.

2. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

3. Soweit die beim Auftragnehmer getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich. Entsprechendes gilt für Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie bei Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten.

§ 10 Sonstiges

1. Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

2. Der Gerichtsstand für beide Parteien ist der Sitz des Auftragnehmers.

3. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Für den Auftraggeber	**Für den Auftragnehmer**
Ort:	Aschaffenburg
Unterschrift: _____	_____
Name:	Name: **Ulrich Eymann**
Position:	Geschäftsführer
Datum:	Datum: ...
	_____
	Name: **ppa. Michael Weis**
	Prokurist / Leiter IT-Services
	Datum: ...