Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag nach Art. 28 Abs.3 Datenschutz-Grundverordnung (DS-GVO) (Auftragsdatenverarbeitung)

Zwischen

Kunden der Zmail GmbH
(z.B. Werbetreibende Unternehmen, Agenturen und andere Werbevermittler)
- nachfolgend **Auftraggeber** genannt –

und der

Zmail GmbH, Luitpoldstrasse 76a 91052 Erlangen
- nachfolgend **Auftragnehmer** genannt –

1. Präambel
Der Abschluss dieser Vereinbarung über die Verarbeitung von Daten im Auftrag erfolgt im Lichte der europäischen Datenschutzgrundverordnung (DSGVO), die ab dem 25. Mai 2018 in Kraft tritt. Vor diesem Hintergrund schließen die Parteien die nachstehende Vereinbarung, um sicherzustellen, dass die Datenverarbeitung zur Leistungserbringung auch zukünftig rechtskonform durchgeführt werden kann.
Der Auftraggeber betraut den Auftragnehmer mit der Verarbeitung personenbezogener Daten. Für diese Auftragsverarbeitung im Sinne von Art. 28 der Datenschutz-Grundverordnung (DS-GVO) gelten die Regelungen dieser Vereinbarung.

2. Gegenstand und Dauer des Auftrags

Gegenstand des Auftrags
Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:
- Durchführung von performance-orientierten Email-Versendungen an Adressbestände des Auftragsverarbeiters

Dauer des Auftrags
Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von 30 Tagen zum Monatsende gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

3. Konkretisierung des Auftragsinhalts

Art und Zweck der vorgesehenen Verarbeitung von Daten

Der Auftraggeber liefert vor der Durchführung einer Email-Versendung regelmäßig Blacklisten mit Email-Adressen an. Die darin enthaltenen Email-Adressen werden durch den Auftragsverarbeiter von den Versendungen ausgeschlossen. Es kann zudem vorkommen, dass vor der Durchführung einer

Email-Kampagne eine durch den Auftraggeber angelieferte Kundenliste gegen den Kundenbestand des Auftragsverarbeiters abgeglichen werden muss, z.B. um Bestandskunden von der werblichen Ansprache auszuschließen.

a) **Ort der Datenvereinbarung:** Die vertraglich vereinbarte Dienstleistung wird grundsätzlich und ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen gesetzlichen Voraussetzungen erfüllt sind.

b) Die Anlieferung der Blacklisten und Kundenlisten erfolgen durch den Auftraggeber gemäß den aktuell geltenden Datenschutzverordnungen und organisatorische/technische Maßnahmen hierzu sind in vollem Maße in der Verantwortung des Auftraggebers.

Art der Daten
Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten / -kategorien
- Personenstammdaten (z.B. Anrede, Vorname, Name, Strasse, Hausnummer, PLZ, Ort)
- Kommunikationsdaten (z.B. Email)

Kategorien betroffener Personen
Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:
- Kunden
- Interessenten
- Werbesperren
- frühere Beschwerdeführer

4. Technisch-organisatorische Maßnahmen

a) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung einmalig als Standardprozess zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben.

Bei Annahme des Auftrags durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

b) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 EU-DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 EU-DSGVO herzustellen, soweit in seinem Einflussbereich. 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-DSGVO zu berücksichtigen.

c) 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 einmalig als Standardprozess zu dokumentieren.

5. Berichtigung, Einschränkung und Löschung von Daten

a) 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. Ausgenommen hiervon sind Blacklisten, Beschwerdelisten, Kundenlisten u.a. die beim Auftragnehmer grundsätzlich nach Abwicklung des Auftrags ohne Weisung des Auftraggebers gelöscht werden.
Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten, sobald der Auftraggeber dem Auftragnehmer einen den Anforderungen des Datenschutzgesetzes konformen Kommunikationskanal zur Verfügung stellt (z.B. Login mit Zugangsdaten).

b) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

6. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

1. Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

2. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format (E-Mail ist ausreichend) festzulegen.

3. Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen schriftlich oder in einem dokumentierten elektronischen Format (E-Mail ist ausreichend). Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

4. Der Auftraggeber ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

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

6. Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

7. Der Auftraggeber trägt die Verantwortung für die Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung. Dies betrifft auch die Verpflichtung der Auftraggeber nach dem Gesetz gegen unlauteren Wettbewerb (insbesondere zur Einholung einer Einwilligung nach § 7 UWG) und dem Fernmeldegeheimnis gemäß Telekommunikationsgesetz (§ 88 TKG). Der Auftragnehmer weist darauf hin, dass keine Werbung unter Verstoß gegen gesetzliche Vorschriften durch die Auftraggeber versandt werden darf.

8. Verantwortlichkeit für Datenverarbeitung; Auftraggeber trägt die Verantwortung für die Verarbeitung und ist gegenüber Dritten für die Einhaltung der Vorschriften der Datenschutzgesetze verantwortlich. Auftraggeber hat die datenschutzrechtliche Zulässigkeit der Auftragsdatenverarbeitung und des Auftrags eigenverantwortlich selbst zu beurteilen. Ist Auftraggeber der Meinung, die Verarbeitung durch den Auftragnehmer verstoße gegen Pflichten von Auftraggeber, so hat er den Auftragnehmer hierauf hinzuweisen und eine rechtskonforme Datenverarbeitung durch entsprechende Weisungen sicherzustellen.

9. Auftraggeber ist allein für die rechtmäßige Erhebung der Daten (Einwilligung durch Double-Opt-In Verfahren oder gemäß §7 Abs. 3 UWG etc.) und die sichere Übermittlung der Daten an den Auftragnehmer zum Zwecke der Datenverarbeitung im Umfang dieser Vereinbarung verantwortlich. Der Auftraggeber sichert zu, nur solche Daten von seinen Kunden und Nutzern zu erheben und dem Auftragnehmer zur Verfügung zu stellen, die ausdrücklich zu einer solchen Erhebung, Verarbeitung und ggf. einer Auswertung eingewilligt haben. Insbesondere ist dem Auftraggeber bewusst, dass eine Auswertung personenbezogener Daten (z.B. Response-Daten wie Öffnungen und Klicks) eines Empfängers im Rahmen eines sog. Trackings nur möglich ist, wenn Auftraggeber den Auftragnehmer bestätigt, dass ihm von jeweiligen Empfänger die Einwilligung für die Auswertung der personenbezogenen Daten vorliegt.

10. Mitteilungs- und Weisungspflichten: Im Falle eines unmittelbaren Auskunftsverlangens, Hinweises, einer Warnung oder Anweisung der Aufsichtsbehörde gemäß Art. 58 DSGVO hat Auftraggeber den Auftragnehmer zu unterstützen und sicherzustellen, dass dem behördlichen Verlangen im Einklang mit dieser Vereinbarung Folge geleistet werden kann.

7. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

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

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 EU-DSGVO ausübt sofern er dazu verpflichtet ist.
- Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.
- Bestellte(r) Datenschutzbeauftragte(r) ist dem Auftraggeber mit vollständigem Namen und Kontaktdaten mitzuteilen [Anrede, Vorname, Name, Organisationseinheit, Telefon, E-Mail]. Ein

Wechsel des Datenschutzbeauftragten ist dem Auftraggeber ebenfalls unverzüglich mitzuteilen.
- Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

b) Insofern der Auftragnehmer nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet ist wird dem Auftraggeber beim Auftragnehmer ein Ansprechpartner mit vollständigem Namen und Kontaktdaten mitgeteilt [Anrede, Vorname, Name, Organisationseinheit, Telefon, E-Mail].

c) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 EU-DSGVO.
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. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

d) Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechend Art. 28 Abs. 3 S. 2 lit. c, 32 E-DSGVO

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

f) Die unverzügliche Information des Auftraggebers 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.

g) 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.

h) Soweit der Auftragnehmer seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit Auftrag beim Auftraggeber ausgesetzt ist, hat ihn der Auftraggeber uneingeschränkt und kostenfrei dienlich zu sein.

i) 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 Person gewährleistet wird.

j) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse.

k) Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder

Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).

l) Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.

m) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen
Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

n) Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

o) Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz- Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).

p) Der Auftragnehmer wird den Auftraggeber darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

q) Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

r) Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

s) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig

machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Aufragnehmer stehen, hat der Auftragnehmer gegen dieses ein Einspruchsrecht.

t) Kosten die dem Auftragnehmer durch seine Unterstützungshandlung entstehen, sind ihm im angemessenen Umfang zu erstatten. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

u) Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind. Er sicher weiter zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DS-GVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

8. Weisungsberechtigte des Auftraggebers und des Auftragnehmers

a. Sowohl Auftraggeber und Auftragnehmer teilen den jeweiligen Weisungsberechtigten bzw. Weisungsempfänger mit vollständigen Kontaktdaten mit.
b. Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind den Vertragspartnern unverzüglich und grundsätzlich schriftlich (E-Mail ist ausreichend) die Nachfolger bzw. die Vertreter mitzuteilen.

8. Unterauftragsverhältnisse

a) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen.
Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer 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 zu treffen sowie Kontrollmaßnahmen zu ergreifen.

b) Der Auftragnehmer darf Unterauftragnehmer nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen. Ausgeschlossen hiervon sind technische Dienstleister mit Sitz innerhalb der EU.

c) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

d) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU / des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

e) Eine weitere Auslagerung durch den Unterauftragnehmer ist nicht gestattet; Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

f) Zurzeit sind für den Auftragnehmer die in **ANHANG 2** mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

g) Der Auftragsverarbeiter informiert den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DS-GVO).

9. Kontrollrechte des Auftraggebers

a) 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.

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

c) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch:
- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 EU-DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 EU-DSGVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Datenschutzbeauftragter, IT-Sicherheitsabteilung)
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz)
- oder weitere geeignete Maßnahmen gemäß Entscheidung des Auftragnehmers

10. Unterstützung des Auftraggebers bei der Einhaltung dessen Pflichten

a) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der EU-DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, zur Meldepflichten bei Datenpannen, zur Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören insbesondere

- die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
- die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden,
- die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen,
- die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung und
- die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

b) Für Unterstützungsleistungen soll der Auftragnehmer eine Vergütung beanspruchen.

11. Weisungsbefugnis des Auftraggebers

a) Mündliche Weisungen wird der Auftraggeber unverzüglich in Textform bestätigen.

b) Der Auftraggeber hat den Auftragnehmer unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftraggeber ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird.

12. Löschung von Daten und Rückgabe von Datenträgern

a) 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 Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

b) Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial.

c) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

13. Haftung

Der Auftragnehmer haftet gegenüber dem Auftraggeber nur im Rahmen des ARt.82 abs.2 s.2 DSGVO und nur dann, wenn der Auftragnehmer schuldhaft eine ihr durch die DSGVO auferlegte Pflicht verletzt.

Eine Haftung des Auftragnehmers ist weiterhin ausgeschlossen, soweit die Pflichtverletzung durch den Auftraggeber verschuldet wurde. Insbesondere haftet Auftragnehmer gegenüber nicht in Fällen, in denen die mit AG abgestimmten technischen und organisatorischen Maßnahmen des Auftragnehmers deshalb nicht den Anforderungen nach Art. 32 DSGVO entsprechen, weil Auftraggeber seinen Informationspflichten nach 3.3.2 nicht oder nicht rechtzeitig nachkommt.

Soweit eine Haftung des Auftragnehmers nach den obigen Ziffern ganz oder teilweise ausgeschlossen ist, stellt Auftraggeber den Auftragnehmer auf erstes Anfordern von allen Ansprüchen frei, die Dritte wegen der Datenverarbeitung im Auftrag von Auftraggeber gegen den Auftragnehmer erheben und übernimmt hierbei die Kosten der notwendigen Rechtsverteidigung einschließlich sämtlicher Gerichts- und Anwaltskosten in gesetzlicher Höhe. Ebenso wie fakultative Kosten des Auftragnehmers in diesem Zusammenhang.

Das Gleiche gilt, soweit eine Inanspruchnahme durch Dritte aufgrund der Erhebung oder Übermittlung Ihrer Daten an Auftragnehmer oder aufgrund der Auswertung der Daten im Rahmen des Trackings erfolgt, oder eine Inanspruchnahme durch Dritte den auf Auftragnehmer entfallenden Verschuldensanteil bei einer gesamtschuldnerischen Haftung summenmäßig übersteigt. Auftraggeber ist verpflichtet Auftragnehmer in angemessener Weise bei der Verteidigung gegenüber den von Dritten erhobenen Ansprüchen zu unterstützen, unverzüglich, wahrheitsgemäß und vollständig alle Informationen zur Verfügung zu stellen, die für die Prüfung der Ansprüche und eine Verteidigung erforderlich sein könnten und alle geeigneten Beweismittel dem Auftragnehmer zugänglich zu machen.

Die Haftung von Auftraggeber und Auftragnehmer bestimmt sich im Außen- und Innenverhältnis nach den Vorgaben des Art. 82 EU-DSGVO.

Für die Haftung gilt die entsprechende Regelung der AGB des Auftragnehmers.

14. Unterzeichnung

Diese Vereinbarung gilt bei Auftragserteilung ohne Unterschrift zwischen Auftraggeber und Auftragnehmer als ausdrücklich angenommen.
Die aktuelle Vereinbarung ist jederzeit auf der Homepage des Auftragnehmers einsehbar unter www.zmail.de

ANHANG I: Subunternehmer
ANHANG II: Technisch-organisatorische Maßnahmen

ANHANG I: Subunternehmer

Die Vertraglich vereinbarten Leistungen werden unter Einschaltung von Subunternehmen durchgeführt, die in diese Verarbeitung mit einbezogen sind.

Nachstehend werden alle Subunternehmen aufgeführt, die unmittelbar mit der Leistungserstellung für den Auftraggeber beteiligt sind und möglicherweise Zugriff auf die Daten des AG haben oder haben können. Dazu zählen auch externe IT-Dienstleister mit entsprechenden Zugriffsrechten.

Subunternehmer

1. **Episerver GmbH** - Wallstraße 16, 10179 Berlin, Deutschland
   Email: infodach@episerver.com | Tel.: +49 (0)30 7680780 | Web: www.episerver.com
   Hauptniederlassung Europa: Episerver AB, Regeringsgatan 67, Box 7007, 103 86 Stockholm, Schweden E-Mail: info@episerver.com Telefon: +46 8 55 58 27 00
   Leistungsbeschreibung: Emailversandlösung

2. **Webanizer AG** - Schulgasse 5, 84359 Simbach am Inn, Deutschland
   Email: service@sendeffect.de | Tel.: +49 (0) 8571 - 97 39 69-0 | Web: www.sendeffect.de
   Leistungsbeschreibung: Emailversandlösung

3. **Beyond Relationship Marketing GmbH** - Wendenstrasse 21B, 20097 Hamburg, Deutschland
   Email: contact@beyondrm.com | Tel: +49 (0)40 3600 68 48 | Web: www.beyondrm.de
   Leistungsbeschreibung: Emailversandlösung

4. **Host Europe GmbH** - Hansestrasse 111, 51149 Köln, Deutschland
   Email: info@hosteurope.de | Tel.: +49 (0) 2203 9934 1040 | Web: www.hosteurope.de
   Leistungsbeschreibung: Hosting

5. **1&1 Internet SE**, Elgendorfer Str. 57, 56410 Montabaur, Deutschland
   Email: info@1und1.de | Tel: +49 (0) 721 96 00 | Web: www.1und1.de
   Leistungsbeschreibung: Hosting

6. **Microsoft Deutschland GmbH** - Walter-Gropius-Straße 5, 80807 München, Deutschland
   Tel.: +49 (0) 89 31 76 0 | Fax: +49 (0) 89 31 76 1000 | Web: www.microsoft.com/de-de/
   Leistungsbeschreibung: Hosting

ANHANG II: Technische und organisatorische Maßnahmen des Auftragnehmers

Der Auftragnehmer betreibt kein eigenes Rechenzentrum. Sämtliche personenbezogenen Daten werden auf den Infrastrukturen der Subunternehmer und derer spezialisierten IT-Dienstleister mit Sitz innerhalb der Europäischen Union gespeichert und verarbeitet (siehe ANHANG I).

Der Auftragnehmer trifft in seinem Bürogebäude nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.

1. Vertraulichkeit

Zutrittskontrolle
Verwehrung des Zugangs zu Verarbeitungsanlagen für Unbefugte, mit denen die Verarbeitung durchgeführt wird.
Maßnahmen:
- Festlegung befugter Personen: es besteht eine klare Regelung zu befugten Personen.
- Empfang mit Besucherregelung: Zugang in die Büroräume nur durch befugte Personen ermöglicht. Zugangs- und Verweilkontrolle bis zum Verlassen der Räumlichkeiten.
- Schlüsselregelung und aktuelle Schlüsselliste
- Verschlossene Bürotüren und Fenster bei Abwesenheit. Haupteingang elektronisch gesichert und verschlossen.
- Objektsicherung und gesicherter Eingang für An- und Ablieferung: Zugang im 2. Obergeschoss. 2 verschlossene Haupttüren.
- Closed Shop Betrieb: kein Publikumsverkehr im Bereich der Datenverarbeitung.

Zugangskontrolle
Das Eindringen Unbefugter in die DV-Systeme wird durch technische (Kennwort- und Passwort-Schutz) und organisatorische (Benutzerverwaltung) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung verhindert
Maßnahmen:
- Kennwortverfahren (u.a. Passwortkomplexität, Mindestlänge, regelmässige Überprüfung und Wechsel des Kennworts)
- Automatische Sperrung (z.B. Kennwort oder Pausenschaltung)
- Einrichtung eines Benutzerstammsatzes pro User
- Verschlüsselung von Datenträgern
- Berechtigungen zum Zugang zu Daten oder Systemen werden von einer zentralen Stelle vergeben
- Mobile IT-Systeme und mobile Datenträger nicht erlaubt
- IT-Systeme werden durch 2 Programme vor Viren und Schadsoftware geschützt
- unberechtigte Zugriffe von Dritten auf IT-Systeme werden durch Firewall erkannt und unterbunden

Zugriffskontrolle
Es werden Maßnahmen ergriffen die gewährleisten, dass ausschließlich Berechtigte auf Daten des Auftraggebers beim Auftragnehmer zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder

entfernt werden können.

Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung.
Maßnahmen:
- Differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte)
- Regelung zum Passwortgebrauch (regelmäßige Kontrolle und Wechsel, Geheimhaltung)
- Benutzerrollen und Berechtigungen werden alle 6 Monate regelmäßig überprüft
- Zugriffsrechte werden beim Ausscheiden aus dem Unternehmen oder beim Wechsel einer Aufgabe im Unternehmen entzogen
- Anzahl der Administratoren ist auf das Minimum beschränkt
- Zugriffe auf externe Anwendungen werden protokolliert
- Papierunterlagen mit personenbezogenen Daten werden per Schredder sicher vernichtet

Trennungskontrolle
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden durch Mandantenfähigkeit. Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken.
Maßnahmen:
- Mandantenfähigkeit mit Zweckbindung
- Daten verschiedener Kunden werden getrennt voneinander verarbeitet und ein Zugriff von Kunden auf Daten anderer Kunden ist ausgeschlossen

Pseudonymisierung & Verschlüsselung
Eine Pseudonymisierung der personenbezogenen Daten ist nicht möglich, da Kern der Dienstleistung die Nutzung der Email-Adresse ist. Weitere personenbezogene Daten sind nicht nötig (optional). Eine Verschlüsselung der Empfängerdaten ist bei den aktiv in Nutzung befindlichen Daten nicht möglich. Archivierte Empfängerdaten werden verschlüsselt abgelegt.

2. Integrität

Eingabekontrolle
Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder gelöscht worden sind:
- Protokollierungssysteme der externen Anwendungen

Weitergabekontrolle
Es werden Maßnahmen ergriffen um zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stelle eine Übermittlung personenbezogener Daten durch Einrichtung zur Datenübertragung vorgesehen ist.
Maßnahmen:
- Verschlüsselung und Tunnelverbindung durch VPN
- Transportsicherung Pflicht

- Vom Auftragnehmer erteilte Pflicht an Auftraggeber dass Übertragung der personenbezogene Daten zwischen Auftraggeber und Auftragnehmer nur per Login oder verschlüsselt zu erfolgen sind.
- Daten werden direkt nach der Beendigung des Auftrags unwiederbringlich gelöscht

3. Verfügbarkeit und Belastbarkeit

Es wird gewährleistet, dass personenbezogene Daten auf den Systemen des Auftragnehmers gegen zufällige Zerstörung oder Verlust geschützt sind.
Maßnahmen zur Verfügbarkeitskontrolle und zur Abschottung:
- regelmäßiges Backup-Verfahren in der Cloud gewährleistet rasche Datenwiederherstellung
- Virenschutz und Firewall im Einsatz
- Notfallplan
- Intrusion Detektion Systeme und Einsatz aktueller Verschlüsselungsverfahren bei den externen Systemen

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Maßnahmen:
- die Unternehmensleitung Verantwortung für Datenschutz und Informationssicherheit übernommen
- Beschäftigte werden regelmäßig zum Datenschutz geschult (1 Schulungsemail je 6 Monate)
- Beschäftigte wurden zum vertraulichem Umgang mit personenbezogenen Daten verpflichtet (Vertraulichkeitserklärung)
- Datenschutzbeauftragte aufgrund Unternehmensgröße nicht verpflichtend aber stattdessen wurde ein dauerhafter Ansprechpartner für Datenschutz benannt
- durch regelmäßige Schulung der Beschäftigten wird sichergestellt, dass Datenschutzverletzungen erkannt und unverzüglich gemeldet werden
- durch tägliche Prüfung der Anfragen und durch dauerhaft Zuständigen wird sichergestellt, dass Anfragen von Betroffenen fristgemäß bearbeitet werden
- Analyse der weiteren Erfordernisse des DSGVO um die bestehenden Grundlagen zu verbessern und zu erweitern insbesondere in der Implementation und Dokumentation von besseren Prozessen
- Datenschutz-Management vorhanden

Auftragskontrolle

Es erfolgt keine Auftragsdatenverarbeitung ohne entsprechende Weisung des Auftraggebers.
Maßnahmen:
- Eindeutige Vertragsgestaltung
- Formalisierte Auftragserteilung
- Kriterien zur Auswahl des Auftragnehmers
- Kontrolle der Vertragsausführung