



Zusatzvereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

Zwischen der

- Verantwortlicher - nachstehend Auftraggeber genannt -

und der

multi-media-management GmbH
Georgswall 5, 30159 Hannover

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt -

1 Gegenstand und Dauer des Auftrags

1.1 Aus dem Hauptvertrag „Servicevertrag GENOPACE BaufiLead webBank/ #webBank“ ergeben sich Gegenstand und Dauer des Auftrags, sowie Art und Zweck der Verarbeitung. Der Auftragnehmer verarbeitet personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieser Zusatzvereinbarung.

1.2 Art der Daten und Kreis der Betroffenen:

Datenarten:

- Anrede
- Vorname
- Nachname
- Geburtsdatum
- E-Mail-Adresse
- Telefon tagsüber
- Straße
- Hausnummer
- Postleitzahl
- Ort
- Anstellungsverhältnis
- Monatliches Nettoeinkommen
- IP-Adresse

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Interessenten
- Kunden

1.3 Die Zusatzvereinbarung endet mit Beendigung des Hauptvertrages, ohne dass es einer Kündigung bedarf.

Das Recht zur fristlosen, außerordentlichen Kündigung dieser Zusatzvereinbarung aus wichtigem Grund bleibt unberührt.

2 Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung der Daten

2.1 Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung der Daten ergeben sich aus dem zwischen den Vertragsparteien bestehenden Vertrag.

2.2 Die vertraglich vereinbarte Dienstleistung wird ausschließlich in Deutschland, einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z.B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

3 Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

- 3.1 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.
- 3.2 Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.
- 3.3 Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.
- 3.4 Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
- 3.5 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.

4 Pflichten des Auftragnehmers

- 4.1 Der 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).
- 4.2 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.
- 4.3 Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.
- 4.4 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. e und f DS-GVO).
- 4.5 Der Auftragnehmer wird den Auftraggeber unverzüglich 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 so lange auszusetzen, bis sie

durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

- 4.6 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 berechnete Interessen des Auftragnehmers dem nicht entgegenstehen.
- 4.7 Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.
- 4.8 Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechnete ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst zu kontrollieren (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO).
- Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt. Hierzu wird bis auf weiteres folgendes vereinbart: der Aufwand auf Seiten des Auftragnehmers im Rahmen der Prüfung, wird zum aktuellen Stundensatz in Rechnung gestellt. Die Gesamtkosten werden vor der Prüfung in einem Angebot zusammen mit dem Prüfungsumfang festgelegt.
- 4.9 Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind.
- 4.10 Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.
- 4.11 Der Auftragnehmer sichert 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 DSGVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.
- 4.12 Der Auftragnehmer sichert zu, einen fachkundigen betrieblichen Datenschutzbeauftragten bestellt zu haben. Der Datenschutzbeauftragte ist in Anhang 1 aufgeführt. Sämtliche Ansprechpartner sind empfangsberechtigt.
- 4.13 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.
- a) 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
 - b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
 - c) 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

- d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
- e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

5 Technische und organisatorische Maßnahmen

- 5.1 Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DS-GVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

- 5.2 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und einer kontinuierlichen Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, auf alternative angemessene Maßnahmen zurückzugreifen. Dabei darf das Sicherheitsniveau der bestehenden Maßnahme nicht unterschritten werden.

In diesem Rahmen gewährleistet der Auftragnehmer dem Auftraggeber, die Umsetzung aller Maßnahmen gemäß Anhang 2 dieser Zusatzvereinbarung.

6 Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DS-GVO

- 6.1 Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen.
- 6.2 Auf schriftliche Aufforderung durch den Auftraggeber hat der Auftragnehmer sämtliche Daten des Auftraggebers datenschutzgerecht zu löschen. Dies gilt nicht für Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen oder soweit z.B. rechtliche Regelungen, gesetzliche Pflichten oder gerichtliche Verfügungen dem entgegenstehen. Entstehen durch eine Löschung vor Vertragsbeendigung zusätzliche Kosten, so trägt diese der Auftraggeber.

7 Unterauftragsverhältnisse

- 7.1 Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 DS-GVO, welche auf einem der o. g. Kommunikationswege (Ziff. 4) mit Ausnahme der mündlichen Gestattung erfolgen muss. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig auswählt.
- 7.2 Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

- 7.3 Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.
- 7.4 Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO).
- 7.5 Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat.

Der Auftragnehmer hat die Einhaltung der Pflichten des/der Subunternehmer(s) zu überprüfen. Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen.

Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

Zurzeit sind für den Auftragnehmer die folgenden - 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.

Adacor Hosting GmbH

Emmastraße 70a
45130 Essen
(Hosting Services)

- 7.6 Der Auftragsverarbeiter informiert den Verantwortlichen immer 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).

8 Haftung

- 8.1 Auf Art. 82 DS-GVO wird verwiesen.

9 Sonstige Vereinbarungen

- 9.1 Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.
- 9.2 Sollte eine Bestimmung dieses Vertrages ungültig oder undurchsetzbar sein oder werden, so bleiben die übrigen Bestimmungen dieses Vertrages hiervon unberührt. Die Parteien vereinbaren, die ungültige oder undurchsetzbare Bestimmung durch eine gültige und durchsetzbare Bestimmung zu ersetzen, welche wirtschaftlich der Zielsetzung der Parteien am nächsten kommt. Das Gleiche gilt im Falle einer Regelungslücke.
- 9.3 Als Gerichtsstand wird hiermit Hannover vereinbart.

Ort, Datum

Ort, Datum



multi-media-management GmbH
Auftragnehmer

Auftraggeber

Anhang 1

Ansprechpartner

Auftragnehmer:	
<i>Datenschutz- beauftragter:</i>	List & Lohr Datenschutz & Informationssicherheit GmbH Garvensstr. 4, 30519 Hannover Telefon: 0511 49 99 99 600 E-Mail: datenschutz@m-m-m.de
Auftraggeber:	
<i>Ansprechpartner:</i>	

Technisch-organisatorische Maßnahmen nach Art. 32 DS-GVO

Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle

- Sicherheitsschlüssel
- Einbruchshemmende Türen und Fenster
- Schlüsselverzeichnis und Schlüsselregelung
- Sorgfältige Auswahl von Reinigungspersonal und externen Dienstleistern
- Protokollierung von Besuchern, Begleitung durch eigene Mitarbeiter

Zugangskontrolle

- Einsatz einer zentralen Firewall
- Zugang zu Computern nur mit gültigem Benutzerkonto/Passwort
- Individuelle, geheime und komplexe Passwörter
- Vermeidung von der Wiederholung von Passwörtern für andere Dienste/Anwendungen
- Einsatz von Anti-Viren Software
- Remote-Zugang durch VPN-Tunnel mit zentraler Anmeldung
- Automatisierte Sperrung des Bildschirms
- Prozesse für Rechtevergabe/-entzug bei Eintritt, Veränderung und Austritt von Mitarbeitern
- Verpflichtung auf das Datengeheimnis gem.

Zugriffskontrolle

- Berechtigungskonzept und individuelle Vergabe von Benutzerrechten
- Für die Berechtigungen auf Ordner wird das Need-To-Know-Prinzip angewandt
- Erteilung und Nutzung von Administratorenrechten auf das Notwendigste begrenzt
- Überprüfung der Zugriffsberechtigung
- Konzept zur Laufwerksnutzung und –Zuordnung
- Bestandskontrolle für mobile Datenträger
- Datenschutzkonforme Vernichtung von Datenträgern und vertraulichen Unterlagen

Trennungskontrolle

- Trennung von Speicherbereichen nach Kunden und Projekten
- Separierung von Dateien bei Datenbanken
- Logische Datentrennung nach Kunden-/Mandantennummern
- Trennung von Entwicklungs-, Test- und Produktivsystemen

Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Weitergabekontrolle

- Einsatz der Systeme nur im privaten Netzwerk oder über verschlüsselte Verbindungen in öffentlichen Netzwerken (VPN-Tunnel)
- E-Mail-Richtlinie bzw. kein Versand personenbezogener Daten per E-Mail
- Unterlagen und Speichermedien werden datenschutzkonform versandt
- Keine Einsicht auf Bildschirme von außerhalb des Gebäudes möglich
- Sorgfältige Auswahl von Transportpersonal-/Fahrzeugen bzw. sichere Verpackungen

Eingabekontrolle

- Organisatorische Festlegung der Zuständigkeiten für die Eingabe, Zugriffsrechte



- Protokollierung von Eingaben/Änderungen/Löschungen
- Sicherung mehrerer Versionssätze im Rahmen des Backups
- Kontrolle der Dateneingabe

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle

- Einsatz von Rauchmeldern und Feuerlöschern
- Spiegelung von Festplatten
- Redundante Sicherung von Daten und Systemen
- Regelmäßige Überprüfung der Wiederherstellbarkeit
- Einsatz von Firewall, Virens Scanner, Spam-Filter und automatischen Produkt-Updates

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs.1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Datenschutz-Management

- Der Datenschutzbeauftragte prüft mit Hilfe von jährlichen Bestandsanalysen das Unternehmen.

Auftragskontrolle

- Eingesetzte Unterauftragnehmer erhalten ausschließlich solche Daten, die zur Erfüllung der Leistung im Sinne des Auftraggebers erforderlich sind.
- Es werden Zusatzvereinbarungen zur Auftragsverarbeitung mit allen Dienstleistern abgeschlossen.

Kontakt

List + Lohr Datenschutz und Informationssicherheit GmbH
Garvensstraße 4
D-30519 Hannover
T 0511-499999-600
F 0511-499999-649

<https://www.datenschutz-hannover.de>

multi-media-management GmbH
Georgswall 5 – 30159 Hannover

Hannover, 01.03.2023