Auftragsverarbeitungsvertrag

zwischen

Charming Media UG (haftungsbeschrankt)
Im Mediapark 5
50670 Köln
DE

-nachfolgend Auftraggeber-

und

Gesellschaft bürgerlichen Rechts, vertreten durch

Just Viral GmbH & Co. KG
Reinholdstraße 5
21073 Hamburg

und

Marius Gebhardt
Nagelsweg 22
20097 Hamburg

und

Denis Hoeger
Königsallee 61
40215 Düsseldorf

-nachfolgend Auftragnehmer-

über Auftragsdatenverarbeitung i.S.d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO).

Präambel

Dieser Auftragsverarbeitungsvertrag (nachfolgend „*Auftragsverarbeitungsvertrag*“) konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der Auftragsverarbeitung im Rahmen der Vertragserfüllung der Parteien ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem zwischen den Parteien geschlossenen Vertrag (nachfolgend „*Vertrag*“) in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (nachfolgend „*Daten*“) des Auftraggebers verarbeiten.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung. Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung:

Art der Daten	Art und Zweck der Datenverarbeitung	Kategorien betroffener Personen
E-Mail, Name, Passwort (gehasht)	Benutzung des Mitgliederbereichs	Kunden von Kunden (Mitglieder)
E-Mail, Name, Webinar Zeitpunkt	Benutzung des Webinar Video Tools	Webinar Teilnehmer

Variable Daten, können vom Kunden definiert werden	Benutzung des Umfrage Tools	Endnutzer des Umfrage Tools
E-Mail, IP-Adresse, DOI Daten, E-Mail Tags, eigene Datensätze	Versand von E-Mails	E-Mail Kontakte
E-Mail, Name, Passwort (gehasht)	Benutzung der Software	Kunden

Die Laufzeit dieses Auftragsverarbeitungsvertrages richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieses Auftragsverarbeitungsvertrages nicht darüber hinausgehende Verpflichtungen ergeben.

§ 2 Anwendungsbereich und Verantwortlichkeit

1. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DS-GVO).
2. Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

§ 3 Pflichten des Auftragnehmers

1. Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten außer es liegt ein Ausnahmefall im Sinne des Art. 28 Abs. 3 a) DS-GVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.
2. Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.
   Diese technischen und organisatorischen Maßnahmen sind in der beigefügten Anlage 1 aufgelistet.
   Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.
3. Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Artt. 33 bis 36 DS-GVO genannten Pflichten.
4. Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

5. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.
   Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.
6. Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.
7. Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.
8. Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart.
   In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.
9. Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.
   Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.
10. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

§ 4 Pflichten des Auftraggebers

1. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
2. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt §3 Abs. (10) entsprechend.
3. Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

§ 5 Anfragen betroffener Personen

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.

§ 6 Nachweismöglichkeiten

1. Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.
2. 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 Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.
Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung verlangen, wenn diesim Vertrag vereinbart ist. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

3. Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz (2) entsprechend.

§ 7 Subunternehmer (weitere Auftragsverarbeiter)

1. Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.
2. Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.
   Eine Weitergabe von Aufträgen durch den Auftragnehmer im Rahmen der in dem Vertrag vereinbarten Tätigkeiten erfolgt an folgende Subunternehmer:
   - Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen
   - OVH GmbH, Christophstraße 19, 50670 Köln
   - Amazon Web Services EMEA Sàrl, 5 Rue Plaetis L-2338 Luxembourg
   - MongoDB Limited, Building Two, Number One Ballsbridge Dublin 4, Ireland
   - CloudFlare, Inc., San Francisco, US (HQ) 101 Townsend St, San Francisco, USA
3. Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

§ 8 Informationspflichten, Schriftformklausel, Rechtswahl

1. Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „Verantwortlicher“ im Sinne der Datenschutz-Grundverordnung liegen.
2. Änderungen und Ergänzungen dieses Auftragsverarbeitungsvertrages 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.
3. Bei etwaigen Widersprüchen gehen Regelungen dieses Auftragsverarbeitungsvertrages zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieses Auftragsverarbeitungsvertrages unwirksam sein, so berührt dies die Wirksamkeit des Auftragsverarbeitungsvertrages im Übrigen nicht.
4. Es gilt deutsches Recht.

§ 9 Haftung und Schadensersatz

Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

Anhang über technische und organisatorische Maßnahmen nach Art. 32 DS-GVO (vgl. auch § 3 Abs. 2 des Auftragsverarbeitungsvertrages)

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1) Zutrittskontrolle - Folgende implementierte Maßnahmen unseres Dienstleisters Hetzner Online verhindern, dass Unbefugte Zutritt zu den Datenverarbeitungsanlagen haben:

1. elektronisches Zutrittskontrollsystem mit Protokollierung
2. Hochsicherheitszaun um den gesamten Datacenterpark
3. dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation-Kunden für Colocation Racks (jeder Auftraggeber ausschließlich für seinen Colocation Rack)
4. Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
5. 24/7 personelle Besetzung der Rechenzentren
6. Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen

2) Zugangskontrolle - Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zugang zu den Datenverarbeitungssystemen haben.

1. Persönlicher und individueller User-Log-In bei Anmeldung am System bzw. Unternehmensnetzwerk
2. Autorisierungsprozess für Zugangsberechtigungen
3. Begrenzung der befugten Benutzer
4. Single Sign-On
5. Zusätzlicher System-Log-In für bestimmte Anwendungen
6. Firewall

3) Zugriffskontrolle - Folgende implementierte Maßnahmen stellen sicher, dass Unbefugte keinen Zugriff auf personenbezogene Daten haben.

1. Verwaltung und Dokumentation von differenzierten Berechtigungen
2. Abschluss von Verträgen zur Auftragsdatenverarbeitung für die externe Pflege, Wartung und Reparatur von Datenverarbeitungsanlagen, sofern bei der Fernwartung die Verarbeitung von personenbezogenen Daten Gegenstand der Dienstleistung ist.
3. Auswertungen/Protokollierungen von Datenverarbeitungen
4. Autorisierungsprozess für Berechtigungen
5. Genehmigungsroutinen
6. Profile/Rollen
7. Maßnahmen zur Verhinderung unbefugten Überspielens von Daten auf extern verwendbare Datenträger (z.B. Kopierschutz, Sperrung von USB-Ports, “Data Loss Prevention (DLP)-System”)

4) Trennungskontrolle - Folgende Maßnahmen stellen sicher, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden.

1. Zugriffsberechtigungen nach funktioneller Zuständigkeit
2. Getrennte Datenverarbeitung durch differenzierende Zugriffsregelungen
3. Mandantenfähigkeit von IT-Systemen
4. Verwendung von Testdaten
5. Trennung von Entwicklungs- und Produktionsumgebung

2. Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

3. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

1) Weitergabekontrolle - Es ist sichergestellt, dass personenbezogene Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und überprüft werden kann, welche Personen oder Stellen personenbezogene Daten erhalten haben. Zur Sicherstellung sind folgende Maßnahmen implementiert:

1. Verschlüsselung von Email bzw.- Email-Anhängen (z.B. WinZip)
2. Verschlüsselung des Speichermediums von Laptops
3. Gesicherter File Transfer (z.B. sftp)
4. Gesicherter Datentransport (z.B. SSL, ftps, TLS)
5. Elektronische Signatur
6. Gesichertes WLAN

2) Eingabekontrolle - Durch folgende Maßnahmen ist sichergestellt, dass geprüft werden kann, wer personenbezogene Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat.

1. Zugriffsrechte
2. Systemseitige Protokollierungen
3. Dokumenten Management System (DMS) mit Änderungshistorie
4. Sicherheits-/Protokollierungssoftware
5. Funktionelle Verantwortlichkeiten, organisatorisch festgelegte Zuständigkeiten
6. Mehraugenprinzip
7. “Data Loss Prevention (DLP)-System”

4. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Verfügbarkeitskontrolle und Belastbarkeitskontrolle - Durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt und für den Auftraggeber stets verfügbar sind.

1. Sicherheitskonzept für Software- und IT-Anwendungen
2. Back-Up Verfahren
3. Aufbewahrungsprozess für Back-Ups (brandgeschützter Safe, getrennter Brandabschnitt, etc.)
4. Gewährleistung der Datenspeicherung im gesicherten Netzwerk
5. Bedarfsgerechtes Einspielen von Sicherheits-Updates
6. Spiegeln von Festplatten
7. Einrichtung einer unterbrechungsfreien Stromversorgung (USV)
8. Klimatisierter Serverraum
9. Virenschutz
10. Firewall

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

1) Datenschutz-Management - Folgende Maßnahmen sollen gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist:

1. Interne Datenschutz-Richtlinie
2. Richtlinien/Anweisungen zur Gewährleistung von technisch-organisatorischen Maßnahmen zur Datensicherheit
3. Verpflichtung der Mitarbeiter auf das Datengeheimnis
4. Hinreichende Schulungen der Mitarbeiter in Datenschutzangelegenheiten
5. Führen einer Übersicht über Verarbeitungstätigkeiten (Art. 30 DSGVO)
6. Durchführung von Datenschutzfolgenabschätzungen, soweit erforderlich (Art. 35 DSGVO)

2) Incident-Response-Management - Folgende Maßnahmen sollen gewährleisten, dass im Fall von Datenschutzverstößen Meldeprozesse ausgelöst werden:

1. Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Aufsichtsbehörden (Art. 33 DSGVO)
2. Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Betroffenen (Art. 34 DSGVO)

6. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

1) Die default Einstellungen sind sowohl bei den standardisierten Voreinstellungen von Systemen und Apps als auch bei der Einrichtung der Datenverarbeitungsverfahren zu berücksichtigen. In dieser Phase werden Funktionen und Rechte konkret konfiguriert, wird im Hinblick auf Datenminimierung die Zulässigkeit bzw. Unzulässigkeit bestimmter Eingaben bzw. von Eingabemöglichkeiten (z. B. von Freitexten) festgelegt und über die Verfügbarkeit von Nutzungsfunktionen entschieden (z. B. hinsichtlich des Umfangs der Verarbeitung). Ebenso werden die Art und der Umfang des Personenbezugs bzw. der Anonymisierung (z. B. bei Selektions-, Export- und Auswertungsfunktionen, die festgelegt und voreingestellt oder frei gestaltbar zur Verfügung gestellt werden können) oder die Verfügbarkeit von bestimmten Verarbeitungsfunktionen, Protokollierungen etc. festgelegt.

7. Auftragskontrolle

Durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten nur entsprechend der Weisungen verarbeitet werden können.

1. Vereinbarung zur Auftragsverarbeitung mit Regelungen zu den Rechten und Pflichten des Auftragnehmers und Auftraggebers
2. Prozess zur Erteilung und/oder Befolgung von Weisungen
3. Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern