

Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 Datenschutz-Grundverordnung

zwischen

Firma: _____
Anschrift: _____
PLZ & Ort: _____
Land: _____

Ansprechpartner: _____
Vor-/Nachname: _____

-im folgenden **Auftraggeber** genannt-

und

contentbird GmbH, Knesebeckstr. 59-61, 10719 Berlin
vertreten durch: Bastian Bickelhaupt und Nicolai Kuban

- im Folgenden **Auftragnehmer** genannt-

Präambel

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im Vertragsverhältnis in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

- 1) Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung. Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den Bestimmungen dieser Anlage nicht darüber hinausgehende Verpflichtungen ergeben. Beginn dieser Anlage ist frühestens der 25.05.2018 und endet mit der Beendigung des Hauptvertrages. Die Verpflichtung zur Verschwiegenheit besteht auch über die Vertragslaufzeit hinweg.
- 2) Bei den zu verarbeitenden personenbezogenen Daten handelt es sich um folgende Arten:

In der Software „contentbird“ angelegte Mitarbeiter und Kontakte des Auftraggebers, an der DMCA (Digital Content Marketing Academy) teilnehmende Mitarbeiter des Auftraggebers, sowie für die Bereitstellung von Downloadprodukten (z.B. Whitepaper) abgefragte Kontaktdaten, d.h. personenbezogene Daten wie: Vorname, Nachname, geschäftliche E-Mail-Adresse, geschäftliche Telefonnummer, Anschrift, Position im Unternehmen, Zahlungsdaten, Social Media Accounts, letzter Login.
- 3) Folgende Kategorien von Personen sind durch die Verarbeitung betroffen: Kunden und Mitarbeiter, sowie durch den Auftraggeber angelegte Kontakte in der Software „contentbird“.

§ 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 DSGVO).
- 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 Artikel 28 Abs. 3 a) DSGVO 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 DSGVO) 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.

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 DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten.
- 4) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter 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) DSGVO 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.
- 10) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, 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 DSGVO, gilt §3 Abs. 10 entsprechend.
- 3) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen. Die Weisungsberechtigten sind in Anlage 2 definiert.

§ 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 dies im 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. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 7 Subunternehmer (weitere Auftragsverarbeiter)

- 1) Hiermit genehmigt der Auftraggeber die Beauftragung von Subunternehmern durch den Auftragnehmer zur Durchführung des Vertragsverhältnisses.
- 2) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

- 3) Dem Auftraggeber sind Kontroll- und Überprüfungsrechte entsprechend § 6 einzuräumen. Durch schriftliche Aufforderung oder Aufforderung in Textform ist der Auftraggeber berechtigt, vom Auftragnehmer Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Subunternehmers zu erhalten.
- 4) Ein Subunternehmerverhältnis liegt nicht vor, wenn der Auftragnehmer Dritte im Rahmen einer Nebenleistung zur Hauptleistung beauftragt, wie beispielsweise bei externem Personal, Post- und Versanddienstleistungen oder Wartung. Der Auftragnehmer wird mit diesem Dritten im erforderlichen Umfang Vereinbarungen treffen, um einen angemessenen Datenschutz zu gewährleisten.

§ 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 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.
- 3) Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.
- 4) Es gilt deutsches Recht.

§ 9 Haftung und Schadensersatz

Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

§ 10 Externer Datenschutzbeauftragter

Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb. Beim Auftragnehmer ist als Beauftragter für den Datenschutz bestellt:

IITR Datenschutz GmbH, Dr. Sebastian Kraska, Marienplatz 2, 80331 München
E-Mail: email@iitr.de, Telefon: 089-18917360

Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

§ 10 Ansprechpartner beim Auftragnehmer

Nicolai Kuban, Geschäftsführer
datenschutz@contentbird.io

Unterschriften

Auftraggeber

Name: _____

Position: _____

Unterschrift:

Ort, Datum

Auftragnehmer

Name: Nicolai Kuban

Position: Geschäftsführer

Unterschrift:

Ort, Datum

Anlagen

Anlage 1 – technische und organisatorische Maßnahmen

Anlage 2 – Weisungsberechtigte Personen

Anlage 1 – technische und organisatorische Maßnahmen

Der Auftragsnehmer sichert zu, dass er die nachfolgend beschriebenen Mindestanforderungen im Rahmen seines Datenschutzkonzeptes einhält. Es beschreibt die im Rahmen der Auftragsverarbeitung erforderlichen Maßnahmen beim Auftragsnehmer zum sicheren Umgang mit personenbezogenen Daten. Die Grundlage für dieses Datenschutz-Konzept bilden die EU-Datenschutzgrundverordnung DS-GVO und ggf. weitere von den interessierten Parteien geforderten Maßnahmen. Hierbei orientiert sich der Auftragsnehmer im Wesentlichen an den Vorgaben der Artikel 24, 25 und 32 DS-GVO. Auf Anforderung weist der Auftragsnehmer die Einhaltung entsprechend nach.

1. Vertraulichkeit

1.1 Zutrittskontrolle

Die Räume, in denen die Verarbeitung personenbezogener Daten erfolgt oder Datenverarbeitungsanlagen installiert sind, dürfen nicht frei zugänglich sein. Sie müssen bei Abwesenheit der Mitarbeiter verschlossen sein. Die Zutrittsberechtigungen müssen in einem geregelten Verfahren nach dem „need to know Prinzip“ vergeben und regelmäßig hinsichtlich ihrer Erforderlichkeit überwacht werden. Räume, in denen Datenverarbeitungsanlagen (Rechenzentrum, Server, Netzwerkverteiler usw.) untergebracht sind, müssen besonders Zutrittsgeschützt sein und dürfen nur für Beschäftigte der IT-Administration (ggfs. der Geschäftsleitung) zugänglich sein. Alternativ müssen die Geräte in geeigneten und verschlossenen Schränken untergebracht sein. Besucher und unternehmensfremde Personen müssen in einem dokumentierten Verfahren registriert und innerhalb der Geschäftsräume beaufsichtigt werden.

1.2 Zugangskontrolle

Für jeden Netzwerkbenutzer muss ein persönlich zugeordneter Benutzer mit einem mindestens 10-stelligen Passwort mit Groß- und Kleinbuchstaben, Ziffer und Sonderzeichen eingerichtet sein. Die Nutzer sind systemseitig zu verpflichten, die Passwörter mindestens alle 90 Tage zu verändern. Die Netzwerkbenutzer sind auf die Einhaltung der Benutzerzugangsrichtlinie dokumentiert zu verpflichten. Die Einrichtung, Änderung und der Entzug von Zugangsberechtigungen muss in einen dokumentierten Verfahren erfolgen. Eingerichtete Zugangsberechtigungen müssen regelmäßig hinsichtlich ihrer Erforderlichkeit dokumentiert überprüft werden. Die Netzwerkzugriffe müssen überwacht und protokolliert werden, dies beinhaltet auch nicht erfolgreiche Anmeldeversuche. Ein Netzwerkzugang muss automatisiert nach spätestens 10 Fehlversuchen systemseitig gesperrt werden.

1.3 Zugriffskontrolle

Für die Zugriffe auf personenbezogene Daten muss ein dokumentiertes, rollenbasiertes Berechtigungskonzept vorhanden sein, welches die Zugriffe in der Form einschränkt, dass nur berechtigte Personen auf die für ihre Aufgabe notwendigen personenbezogenen Daten zugreifen können (Minimumprinzip). Die Passwort-Regelungen aus der Zugangskontrolle müssen auch im Rahmen der Zugriffskontrolle umgesetzt werden. Die administrativen Tätigkeiten müssen auf einen kleinen Kreis von Administratoren eingeschränkt sein. Die Tätigkeiten der Administratoren müssen im Rahmen technisch vertretbaren Aufwandes überwacht und protokolliert werden.

1.4 Pseudonymisierung

Auswertungen müssen pseudonymisiert werden, sofern der Personenbezug für das Ergebnis nicht zwingend erforderlich ist.

1.5 Trennungskontrolle

Die Trennung von personenbezogenen Daten muss durch unterschiedliche Speicherorte oder durch eine Mandantentrennung sichergestellt werden.

2. Integrität

2.1 Weitergabekontrolle

Im Rahmen der Weitergabekontrolle muss sichergestellt werden, dass nur berechtigte Personen die personenbezogenen Daten zur Kenntnis nehmen können. Bei einer Übermittlung per E-Mail sind entsprechende Schutzmaßnahmen (z.B. Verschlüsselung der Kommunikation zwischen den Mail-Servern) zu ergreifen. Mobile Geräte oder mobile Speichermedien müssen verschlüsselt werden, wenn auf ihnen personenbezogene Daten gespeichert werden.

2.2 Eingabekontrolle

Die Eingabe, Änderung und Löschung personenbezogener Daten muss dem durchführenden Beschäftigten zugeordnet werden können. Die Änderung und Löschungen von Datensätzen muss systemseitig eingeschränkt sein, damit ein versehentliches Ändern oder Löschen wirksam verhindert wird.

2.3 Auftragskontrolle

Im Rahmen der Auftragskontrolle muss sichergestellt werden, dass die im Auftrag durchgeführten Datenverarbeitungsvorgänge ausschließlich auf Weisung des Auftraggebers erfolgen. Hierzu müssen die mit der Datenverarbeitung Beschäftigten geschult und unterwiesen werden. Die Auftragsverarbeitung muss durch interne Kontrollen überwacht werden. Die Ergebnisse der Kontrollen müssen dokumentiert werden.

Unterauftragnehmer dürfen nur auf Basis der mit dem Auftraggeber vereinbarten Regelungen beauftragt werden. Die Übermittlung oder der Zugriff auf personenbezogene Daten darf erst dann erfolgen, wenn der Unterauftragnehmer eine Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DS-GVO unterzeichnet hat und die Einhaltung der Regelungen des

Datenschutzkonzeptes bestätigt hat. Die Prüfpflicht des Auftragnehmers gegenüber seinem Unterauftragnehmer ergibt sich aus der mit dem Auftraggeber abgeschlossenen Vereinbarung zur Auftragsverarbeitung.

3. Verfügbarkeit und Belastbarkeit

Die Verarbeitung von personenbezogenen Daten muss auf Datenverarbeitungssystemen erfolgen, die einem regelmäßigen und dokumentierten Patch-Management unterliegen. Es dürfen im Netz keine Systeme verbunden sein, die außerhalb der Wartungszyklen der Hersteller sind (insb. kein Windows XP, Windows Server 2003 etc.). Sicherheitsrelevante Patches müssen innerhalb von 72 Stunden nach Bekanntgabe eingespielt werden. Die durchgängige Verfügbarkeit von personenbezogenen Daten muss mittels redundanten Speichermedien und Datensicherungen gemäß dem Stand der Technik gewährleistet werden. Rechenzentren und Serverräume müssen dem Stand der Technik (Temperaturregelung, Brandschutz, Wassereintritt etc.) entsprechen. Die Server müssen über eine unterbrechungsfreie Stromversorgung (USV) verfügen, die ein geregeltes Herunterfahren ohne Datenverlust sicherstellt.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Es muss ein Verfahren zur Überwachung des Datenschutzes im Unternehmen implementiert sein. Dieses muss die Verpflichtung der Beschäftigten auf das Datengeheimnis, die Schulung und Sensibilisierung der Beschäftigten und die regelmäßige Auditierung der Datenverarbeitungsverfahren beinhaltet. Ebenso muss die Dokumentation des für den Auftraggeber durchgeführten Verarbeitungsverfahrens vor Aufnahme der Datenverarbeitung erfolgen. Für Datenschutzverletzungen und die Wahrung der Betroffenenrechte muss ein durchgängiger Meldeprozess und Bearbeitungsprozess eingeführt sein. Dieser muss auch die Information des Auftraggebers beinhalten.

Anlage 2 - Weisungsberechtigte Personen

Folgende Personen sind zur Erteilung und Entgegennahme von Weisungen befugt:

Erteilung:

Vorname Nachname	Ausweisnummer	E-Mailadresse

Entgegennahme:

Nicolai Kuban, Geschäftsführer: kuban@contentbird.io
Bastian Bickelhaupt, Geschäftsführer: bickelhaupt@contentbird.io