

EU-Datenschutz-Grundverordnung DSGVO

Vereinbarung über eine Auftragsdatenverarbeitung nach Art 28 DSGVO

zwischen der

Reach Media GmbH

HRB 179776 B

Kemperplatz 1

10785 Berlin

- nachstehend Dienstleister genannt -

und

- nachstehend Auftraggeber genannt -

Am heutigen Tage wie folgt:

1. Gegenstand der Dienstleistung

1. Der Dienstleister stellt dem Auftraggeber folgende Leistung zur Verfügung:

Eine temporäre Speicherung von Daten in einer Cloud, sowie die Bereitstellung von Daten zum Download durch eine E-Mail oder einen Link des Auftraggebers.

2. Der Auftraggeber übermittelt dem Dienstleister alle zur Übertragung relevanten Informationen, welche zu jedem Zeitpunkt verschlüsselt auf den Festplatten des Servers gespeichert werden.

3. Innerhalb von maximal sieben Tagen werden alle Daten und Datensätze, welche Absender, Empfänger und Speicherort identifizieren, durch den Dienstleister gelöscht.

4. Nach Upload des Senders erhält der Empfänger einen Download-Link der Datei.

2. Dauer der Vereinbarung

1. Die Vereinbarung ist auf unbestimmte Zeit geschlossen und kann von beiden Parteien mit sofortiger gekündigt werden.

3. Pflichten des Auftragnehmers

1. Der Auftragnehmer verpflichtet sich, Daten ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragnehmers eines schriftlichen Auftrages.

2. Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

3. Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat (Einzelheiten sind der Anlage 1 zu entnehmen).
4. Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Person nach Kapitel 3 der DSGVO - Information, Auskunft, Berichtigung und Löschung, Datenübertragung, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall - innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.
5. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten - Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, vorherige Konsultation.
6. Der Auftragnehmer wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten hat.
7. Dem Auftraggeber oder ihm durch beauftragte Dritte wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht ständiger Einsichtnahme und Kontrolle der Datenverarbeitungseinrichtungen gewährt. Der Auftragnehmer verpflichtet sich, dem Auftraggeber alle Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.
8. Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungen und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben oder in dessen Auftrag zu vernichten. Wenn der Auftragnehmer die Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder nach Wunsch des Auftraggebers in dem Format, in dem er die Daten vom Auftraggeber erhalten hat oder in einem anderen gängigen Format zu übermitteln.
9. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

5. Sub-Auftragsverarbeiter

1. Auftragnehmer ist befugt folgendes Unternehmen als Sub-Auftragsverarbeiter hinzuziehen:

- Hosting Provider für den Server-Betrieb: Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen
- Dienstleister für den E-Mailversand: Amazon Web Services, Inc., 410 Terry Avenue North, Seattle WA 98109, United States (Serverstandort: Irland - EU)

Beabsichtigte Änderungen des Sub-Auftragsverarbeiters sind dem Auftraggeber so rechtzeitig schriftlich bekannt zu geben, dass er dies allenfalls untersagen kann. Der Auftragnehmer schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. Dabei ist sicherzustellen, dass der Sub- Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragnehmer auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

6. Geheimhaltungsverpflichtung

1. Alle zur Erfüllung der Dienstleistung relevanten Informationen werden vom Dienstleister streng vertraulich und geheim gehalten.

Berlin, 18.11.2018

Auftraggeber Dienstleister, Markus Balke, Datenschutzbeauftragter

Anlage 1 – Technisch-organisatorische Maßnahmen

1. Vertraulichkeit

1. Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu den Büroräumen, in denen ein Zugriff auf die Datenverarbeitungssysteme im Rechenzentrum besteht mit Schlüssel und Code gesichertes Türschloss. Zutritt nur durch Mitarbeiter, sowie Gesellschafter.
2. Zugangskontrolle: Schutz vor unbefugter Systemnutzung durch mehrere Sicherheitsebenen, Passwörter, Zwei-Faktor-Authentifizierung, SSH Keys.
3. Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, Standard-Berechtigungsprofile auf Basis des "Need-to-Know-Prinzips", Standardprozess für Berechtigungsvergabe, Protokollierung von Zugriffen, periodische Überprüfung der vergebenen Berechtigungen, insbesondere von administrativen Benutzerkonten.
4. Pseudonymisierung, sofern für die jeweilige Datenverarbeitung möglich, werden primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt und gesondert aufbewahrt.
5. Klassifikationsschema für Daten aufgrund von Selbsteinschätzung.
6. Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch Verschlüsselung, bei E-Mail via Digitale Signatur.
7. Eingabekontrolle: Protokollierung des Datenimports.
8. Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung oder Verlust, beispielsweise Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV, Dieselaggregat), Virenschutz, Firewall, Meldewege und Notfallpläne; Security Checks auf Infrastruktur- und Applikationsebene, Mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum, Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern.
9. Lösungsfristen: Sowohl für Daten als auch Metadaten wie Logfiles.
10. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung.
11. Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen.
12. Datenschutzfreundliche Voreinstellungen.

13. Auftragskontrolle: Keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, beispielsweise eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Auftragsverarbeiters (ISO- Zertifizierung, ISMS), Nachkontrollen.