

Storyblok GmbH
Peter-Behrens-Platz 2
4020 Linz, Österreich
ATU72706128



Vereinbarung

über eine

Auftragsverarbeitung nach Art 28 DSGVO

Der Verantwortliche:

Der Auftragsverarbeiter:

Storyblok GmbH
Peter-Behrens-Platz 2
4020 Linz, Österreich

(im Folgenden Auftraggeber)

(im Folgenden Auftragnehmer)

1. GEGENSTAND DER VEREINBARUNG

- (1) Gegenstand dieses Auftrages ist die Durchführung von Datenverarbeitung in Verbindung mit der Storyblok Plattform. Storyblok stellt eine cloudbasierte Web-Applikation für die Wartung von Inhalten zur Verfügung. Diese ermöglicht es den Endkonsumenten auf den Plattformen des Auftraggebers, den eigenen Inhalt für elektronische Medien zu hinterlegen und mittels Email und Passwort für eine spätere Wiederverwendung abzuspeichern. Diese Vereinbarung ist als Ergänzung zu den Allgemeinen Bedingungen "Terms" (<https://www.storyblok.com/terms>), "Acceptable Use Policy (AUP)" (<https://www.storyblok.com/acceptable-use-policy/>) als auch "Privacy Policy" (<https://www.storyblok.com/privacy-policy>) zu verstehen.
- (2) Folgende Datenkategorien werden verarbeitet:
- a. Kontaktdaten
 - b. Kommunikationsdaten
 - c. Verrechnungsdaten
 - d. Adressdaten
 - e. Analysedaten

- f. Bestell- und Abrechnungsdaten
- g. Vertragsdaten

- (3) Folgende Kategorien betroffener Personen werden unterliegen der Verarbeitung:
- a. Kunden der Storyblok Plattform
 - b. Lizenznehmer
 - c. Lieferanten
 - d. Beschäftigte
 - e. Interessierte
 - f. Webseitenbesucher

2. DAUER DER VEREINBARUNG

Die Vereinbarung ist auf unbestimmte Zeit geschlossen und kann von beiden Parteien gekündigt werden. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund, oder bei Verletzung der "Terms" (<https://www.storyblok.com/terms>) durch den Auftraggeber, bleibt unberührt.

3. PFLICHTEN DES AUFTRAGNEHMERS

- (1) Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse 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 III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, 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, Datenschutz-Folgeabschätzung, 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 wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch ihn beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene 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 Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben / 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 herauszugeben.
- (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.

4. ORT DER DURCHFÜHRUNG DER DATENVERARBEITUNG

Datenverarbeitungstätigkeiten werden zumindest zum Teil auch außerhalb der EU bzw des EWR durchgeführt, und zwar in den United States. Das angemessene Datenschutzniveau ergibt sich aus:

- einem Angemessenheitsbeschluss der Europäischen Kommission nach Art 45 DSGVO.
- Standarddatenschutzklauseln nach Art 46 Abs 2 lit c und d DSGVO.

5. SUB-AUFTRAGSVERARBEITER

Der Auftragnehmer ist befugt folgende Unternehmen als Sub-Auftragsverarbeiter hinzuziehen:

| Sub-Auftragsverarbeiter | Land | Service |
|-------------------------|---------------|------------------|
| Amazon Web Services | United States | Hosting Provider |
| Stripe Payment Europe | Ireland | Payment Provider |
| Crisp | France | Chat Provider |
| Hubspot | United States | CRM Provider |

| | | |
|-----------|---------------|--------------------|
| Google | Ireland | Storage Provider |
| Mailchimp | United States | Mail Provider |
| Twilio | United States | Messaging Provider |
| Auth0 | United States | SSO Provider |

Er hat den Auftraggeber von der beabsichtigten Heranziehung eines Sub-Auftragsverarbeiters so rechtzeitig zu verständigen, 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.

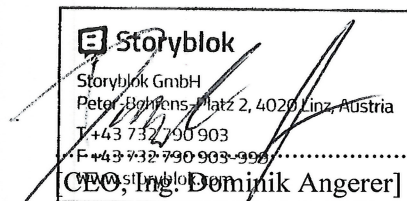
_____, am _____

Linz, am 28.05.2018

Für den Auftraggeber:

Für den Auftragnehmer:

.....
[]



Anlage ./1 – Technisch-organisatorische Maßnahmen

VERTRAULICHKEIT

- **Zutrittskontrolle:** Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, z.B.: Schlüssel, Magnet- oder Chipkarten, elektrische Türöffner, Portier, Sicherheitspersonal, Alarmanlagen, Videoanlagen; Interne Datenverarbeitungsanlagen sind nur für Administrator mit Schlüssel zugänglich und durch Zwei Faktoren Authentifizierung möglich.
- **Zugangskontrolle:** Schutz vor unbefugter Systembenutzung durch Kennwörter (einschließlich entsprechender Policy), automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern; Alle Rechner und Zugänge sind über Kennwörter geschützt. Es gibt fix definierte Mitarbeiter, welche Zugang zur Infrastruktur der Cloud Services besitzen. Diese sind an das Authentifizierungssystem unserer Amazon Accounts gebunden und mittels Zwei Faktoren Authentifizierung abgesichert. Sobald ein Nutzer das Unternehmen verlässt wird dieser Account und somit auch alle weiteren Zugriffsmöglichkeiten deaktiviert.
- **Zugriffskontrolle:** Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen möglich. Zugriff auf Datenbank ist Passwort und via Zwei Faktoren Authentifizierung geschützt. Zugriff auf Server nur über SSH für berechtigte User. Beides nur über internes Netzwerk (ggf. passwort-geschütztes VPN) erreichbar. Vergebene Berechtigungen werden periodisch überprüft. Jegliche Anmeldung/Zugriffe des internen Systems wird protokolliert.
- **Pseudonymisierung:** Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt, und gesondert aufbewahrt.
- **Klassifikationsschema für Daten:** Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

INTEGRITÄT

- **Weitergabekontrolle:** Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;
- **Eingabekontrolle:** Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Automatisierte Protokollierung der Zugriffe und Änderungen werden durchgeführt.

VERFÜGBARKEIT UND BELASTBARKEIT

- **Verfügbarkeitskontrolle:** Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: 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;
- **Rasche Wiederherstellbarkeit;**
- **Löschungsfristen:** Sowohl für Daten selbst als auch Metadaten wie Logfiles, udgl.

VERFAHREN ZUR REGELMÄSSIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

- Datenschutz Management: Wir führen in unregelmäßigen Abständen systemische Sicherheitstests durch einen Drittdienstleister durch. Die Erkenntnisse werden dokumentiert.
- Incident-Response-Management wird ausgeführt und dokumentiert.
- Datenschutzfreundliche Voreinstellungen unserer User: Sämtliche neu erstellten User-Profile sind im default privat.
- Auftragskontrolle: Keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Auftragsverarbeiters (ISO-Zertifizierung, ISMS), Vorabüberzeugungspflicht, Nachkontrollen.