

Auftragsverarbeiter-Vertrag

Auftraggeber (Verantwortlicher):

[Vom Auftraggeber auszufüllen: Name/Firma und vollständige Anschrift]

Auftragnehmer (Auftragsverarbeiter):

Secret Creators GmbH; Klettgauerstr. 67; 8212 Neuhausen am Rheinfall; Schweiz

1. Gegenstand und Dauer der Vereinbarung

Gegenstand des Auftrags ist die Verarbeitung personenbezogener Daten im Zusammenhang mit dem Betrieb und der Bereitstellung einer Link-in-Bio-Plattform für den Auftraggeber. Die Plattform ermöglicht die Bündelung und Darstellung von Links, Inhalten und weiterführenden Informationen über eine individuelle Landingpage des Auftraggebers.

Die Verarbeitung umfasst insbesondere:

- die Bereitstellung, den Betrieb und die technische Wartung der Plattform,
- die Speicherung und Auslieferung der vom Auftraggeber bereitgestellten Inhalte,
- die Verarbeitung von Nutzungs- und Verbindungsdaten, soweit dies für die Bereitstellung und Sicherheit der Plattform erforderlich ist,
- gegebenenfalls die Bereitstellung von Statistik- und Analysefunktionen hinsichtlich der Nutzung der Landingpage, soweit diese vom Auftraggeber aktiviert werden.

Eine Verarbeitung personenbezogener Daten zu eigenen Zwecken des Auftragnehmers erfolgt nicht. Insbesondere erfolgt keine Nutzung der Daten für eigene Marketingzwecke des Auftragnehmers.

Der Auftragnehmer verarbeitet personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO ausschließlich auf Grundlage dieser Vereinbarung und der Weisungen des Auftraggebers.

Ort der Datenverarbeitung

Die vertraglich vereinbarte Dienstleistung wird unter Einsatz des Hosting-Dienstleisters Netlify erbracht. Dabei können personenbezogene Daten insbesondere in den USA verarbeitet werden (Netlify-Region us-east-2, Ohio; statische Inhalte werden über das weltweite Netlify-CDN ausgeliefert). Übermittlungen personenbezogener Daten in Drittländer erfolgen unter Einhaltung der Voraussetzungen der Art. 44 ff. DS-GVO. Für Übermittlungen an Netlify in die USA wird nach den Angaben von Netlify das EU-U.S. Data Privacy Framework herangezogen; ergänzend sieht das Netlify Data Processing Agreement die EU-Standardvertragsklauseln (Durchführungsbeschluss (EU) 2021/914) vor.

Dauer des Auftrags

Die Verarbeitung erfolgt für die Laufzeit des zwischen den Parteien bestehenden Vertrags über die Nutzung der Link-in-Bio-Plattform.

Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt. Der Auftraggeber kann diese Vereinbarung insbesondere dann fristlos kündigen, wenn der Auftragnehmer schwerwiegend gegen datenschutzrechtliche Vorschriften oder die Bestimmungen dieser Vereinbarung verstößt, rechtmäßige Weisungen des Auftraggebers nicht befolgt oder Kontrollrechte des Auftraggebers unberechtigt verweigert. Die Verletzung der sich aus Art. 28 DSGVO ergebenden Pflichten gilt regelmäßig als wichtiger Grund.

Kategorien betroffener Personen

- Besucher der Landingpage,
- Kunden, Interessenten oder Geschäftspartner des Auftraggebers,
- Mitarbeiter oder sonstige Ansprechpartner des Auftraggebers,
- sonstige Personen, deren personenbezogene Daten vom Auftraggeber über die Plattform bereitgestellt werden.

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS- GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen:

Die Verarbeitung personenbezogener Daten erfolgt zum Zweck der Bereitstellung und des Betriebs einer vom Auftraggeber genutzten Link-in-Bio- bzw. Landingpage-Lösung. Hierzu zählen insbesondere das Hosting der Seite, die Speicherung und Bereitstellung der vom Auftraggeber eingestellten Inhalte, die technische Administration der Plattform sowie die Verarbeitung von Nutzungs- und Verbindungsdaten, soweit dies für die Bereitstellung, Sicherheit und Funktionsfähigkeit der Plattform erforderlich ist.

Art der Verarbeitung (entsprechend der Definition von Art. 4 Nr. 2 DS-GVO):

- ☒ Erheben ☐ Anpassung ☒ Offenlegung durch Übermittlung ☐ Einschränkung
- ☒ Erfassen ☒ Veränderung ☐ Verbreitung ☒ Löschen
- ☐ Organisation ☒ Auslesen ☒ andere Form der Bereitstellung ☐ Vernichtung
- ☐ Ordnen ☒ Abfragen ☐ Abgleich
- ☒ Speicherung ☒ Verwendung ☐ Verknüpfung

Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 13, 14 und 15 DSGVO):

☒ „personenbezogene Daten“ nach Art. 4 Nr. 1 DS-GVO

☐ „genetische Daten“ nach Art. 4 Nr. 13 DS-GVO

☐ „biometrische Daten“ nach Art. 4 Nr. 14 DS-GVO

☐ „Gesundheitsdaten“ nach Art. 4 Nr. 15 DS-GVO

Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DS-GVO):

Je nach Nutzung der Plattform können insbesondere folgende Daten verarbeitet werden:

- Stammdaten und Kontaktdaten des Auftraggebers bzw. seiner Ansprechpartner,
- IP-Adressen und technische Verbindungsdaten der Besucher der Landingpage,
- Nutzungsdaten (z. B. Aufrufe, Klicks und Interaktionen auf der Landingpage),
- sonstige personenbezogene Daten, die der Auftraggeber selbst über die Plattform veröffentlicht oder verarbeiten lässt.

Im Detail:

☒ Namen ☐ Merkmale, die Ausdruck der physischen Identität sind

☐ Kennnummer ☐ Merkmale, die Ausdruck der physiologischen Identität sind

☐ Standortdaten ☐ Merkmale, die Ausdruck der genetischen Identität sind

☒ Online-Kennung ☐ Merkmale, die Ausdruck der psychischen Identität sind

☐ Merkmale, die Ausdruck der wirtschaftlichen Identität sind

☐ Merkmale, die Ausdruck der kulturellen Identität sind

☐ Merkmale, die Ausdruck der sozialen Identität sind

2. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

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.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

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.

Der Auftraggeber ist berechtigt, sich wie unter Nr. 5 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

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.

3. Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

Weisungsberechtigte Personen des Auftraggebers sind:

-  Geschäftsleitung des Auftraggebers
-  sowie vom Auftraggeber ausdrücklich benannte Ansprechpartner

Weisungsempfänger beim Auftragnehmer sind:

-  Geschäftsleitung der Secret Creators GmbH
-  sowie intern entsprechend autorisierte Ansprechpartner

Für Weisung zu nutzende Kommunikationskanäle:

- Postadresse des Auftragnehmers

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend

noch für drei volle Kalenderjahre aufzubewahren.

4. Pflichten des Auftragnehmers

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).

Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.

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.

Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

Der Auftragnehmer hat über die gesamte Abwicklung der Dienstleistung für den Auftraggeber insbesondere folgende Überprüfungen in seinem Bereich durchzuführen:

- Regelmäßige Audits

Das Ergebnis der Kontrollen ist zu dokumentieren.

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). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an folgende Stelle des Auftraggebers weiterzuleiten:

- Postadresse des Auftraggebers

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 solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

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 berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

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.

Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (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:

- Einräumung eines Zugangs- und Kontrollrechts, ggf. unter Hinzuziehung eines Datenschutzbeauftragten

Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) ist nur mit Zustimmung des Auftraggebers gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicher zu stellen. Die Maßnahmen nach Art. 32 DS-GVO sind auch in diesem Fall sicherzustellen.

Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind. Er verpflichtet sich, auch folgende für diesen Auftrag relevanten Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen:

KEINE

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.

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.

☐ Beim Auftragnehmer ist als Beauftragte(r) für den Datenschutz Herr/Frau

Vorname: entfällt

Name: entfällt

Organisationseinheit: entfällt

Telefon: entfällt

bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen. oder

☒ Ein betrieblicher Datenschutzbeauftragter ist beim Auftragnehmer nicht bestellt, da die gesetzliche Notwendigkeit für eine Bestellung nicht vorliegt.

5. Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DS-GVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

6. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DS-GVO)

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 diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage

zur Verfügung zu stellen.

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).

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.

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).

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) wie folgt zu überprüfen:

- Überprüfung der TOMs

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 im Anhang 1 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.

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).

7. Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO (Art. 28 Abs. 3 Satz 2 lit. c DS- GVO)

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.

Für die auftragsgemäße Verarbeitung personenbezogener Daten wird eine Methodik zur Risikobewertung verwendet, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten berücksichtigt.

Das im Anhang 2 beschriebene Datenschutzkonzept stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT Systeme und Verarbeitungsprozesse beim Auftragnehmer dar.

Das im Anhang 3 beschriebene Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der datenschutzkonformen Verarbeitung wird als verbindlich festgelegt.

Folgende Möglichkeiten für den Nachweis durch Zertifizierung bestehen:

Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DS-GVO). Das Ergebnis samt vollständigem Auditbericht ist dem Auftraggeber mitzuteilen.

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen.

Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftragnehmer unverzüglich.

Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

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

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, datenschutzgerecht zu löschen bzw. zu vernichten/vernichten zu lassen.

Anhang 1
Subunternehmer

☐ Es werden keine Subunternehmer beschäftigt.

☒ Name: Netlify, Inc.

Anschrift: 101 2nd Street, San Francisco, CA 94105, USA

Auftragsinhalt: Hosting und Auslieferung (CDN), serverseitige Funktionen und
Datenspeicher (Netlify Blobs)

☐ Name:

Anschrift:

Auftragsinhalt:

☐ Name:

Anschrift:

Auftragsinhalt:

☐ Name:

Anschrift:

Auftragsinhalt:

☐ Name:

Anschrift:

Auftragsinhalt:

Anhang 2 - Datenschutzkonzept / Technische und organisatorische Maßnahmen

1. Zugangskontrolle

Eine Umsetzung der technischen und organisatorischen Maßnahmen zur Gewährleistung der Zugangskontrolle ist notwendig. Zugangskontrolle bedeutet die Verwehrung des Zugangs durch Unbefugte zu Verarbeitungsanlagen, mit denen die Verarbeitung von personenbezogenen Daten durchgeführt wird. Folgende Maßnahmen wurden von uns getroffen:

- | | |
|--|--|
| ☐ Alarmanlage | ☐ Personenkontrolle beim Pfortner / Empfang |
| ☐ Absicherung von Gebäudeschächten | ☐ Protokollierung der Besucher |
| ☐ Automatisches Zugangskontrollsystem | ☐ Sorgfältige Auswahl von Reinigungspersonal |
| ☐ Chipkarten, Transponder | ☐ Sorgfältige Auswahl von Wachpersonal |
| ☐ Schließsystem mit Codesperre | ☐ Tragepflicht von Berechtigungsausweisen |
| ☐ Manuelles Schließsystem | ☐ Zugangskonzept |
| ☐ Biometrische Zugangssperren | ☐ Abschließbare Serverschränke |
| ☐ Videoüberwachung der Zugänge | ☐ Türen mit einem Knauf an der Außenseite |
| ☐ Lichtschranken / Bewegungsmelder | ☐ Besucher: Nur in Begleitung durch Mitarbeiter |
| ☐ Sicherheitsschlösser | ☐ |
| ☐ Schlüsselregelung | ☐ |
| ☐ Klingelanlage mit Kamera | |

2. Datenträgerkontrolle

Zudem ist die Umsetzung technischer und organisatorischer Maßnahmen zur Sicherstellung der Datenträgerkontrolle erforderlich. Unter Datenträgerkontrolle versteht man eine Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern. Hierfür wurden von uns folgende Maßnahmen getroffen:

- | | |
|---|---|
| ☐ Verschlüsselung von Datenträgern | ☐ Ordnungsgemäße Vernichtung von Datenträgern |
| ☐ Erstellung eines Berechtigungskonzepts | (nach DIN 66399) |
| ☐ Verwaltung der Rechte durch einen Systemadministrator | ☐ Physische Löschung von Datenträgern vor jeder Wiederverwendung |
| ☐ Beschränkung der Anzahl der Administratoren | ☐ Einsatz von Aktenvernichtern |
| ☐ Passwortrichtlinie inkl. Passwortlänge und Passwortwechsel | ☐ Protokollierung der Vernichtung |
| ☐ Protokollierung von Zugriffen auf | ☐ Sichere Datenlöschung |
| | ☐ VPN Tunnel |
| | ☐ Weitergabe von Daten in anonymisierter |

oder Anwendungen, insbesondere bei der pseudonymisierten Form
Eingabe, Änderung und Löschung von Daten

- ☐ Sichere Aufbewahrung von Datenträgern
- ☐ Physische Löschung von Datenträgern
vor jeder Wiederverwendung

3. Speicherkontrolle

Weiterhin ist die Umsetzung technischer und organisatorischer Maßnahmen zur Sicherstellung der Speicherkontrolle erforderlich. Hierunter versteht man eine Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten. Hierfür haben wir folgende Maßnahmen getroffen:

- | | |
|--|--|
| ☐ Verschlüsselung von Datenträgern | ☐ Sichere Aufbewahrung von Datenträgern |
| ☐ Erstellung eines Berechtigungskonzepts | ☐ Physische Löschung von Datenträgern vor jeder |
| ☐ Verwaltung der Rechte durch einen | Wiederverwendung |
| Systemadministrator | ☐ Ordnungsgemäße Vernichtung von Datenträgern |
| ☐ Beschränkung der Anzahl der | (nach DIN 66399) |
| Administratoren | ☐ Einsatz von Aktenvernichtern |
| ☐ Passworthrichtlinie inkl. Passwortlänge und | ☐ Protokollierung der Vernichtung |
| Passwortwechsel | ☐ Sichere Datenlöschung |
| ☐ Protokollierung von Zugriffen auf | ☐ Anwendungen, insbesondere bei der Eingabe, |
| ☐ Änderung und Löschung von Daten | ☐ |

4. Benutzerkontrolle

Ferner ist die Umsetzung technischer und organisatorischer Maßnahmen zur Sicherstellung der Benutzerkontrolle erforderlich. Unter Benutzerkontrolle versteht man die Verhinderung der unbefugten Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung. Hierfür wurden von uns folgende Maßnahmen getroffen:

- | | |
|--|--|
| ☐ Verschlüsselung von Datenträgern | ☐ Zuordnung von Benutzerprofilen zu IT-Systemen |
| ☐ Festlegung von Datenbankrechten | ☐ Einsatz von Anti-Viren-Software |
| ☐ VPN | ☐ Firewall |
| ☐ Protokollierung der Eingabe, Änderung und | ☐ Einsatz eines Intrusion Detection Systems |
| Löschung von Daten | ☐ Mobile Device Management |
| ☐ Passworthrichtlinie inkl. Passwortlänge und | ☐ Mobile Device Policy |

- | | |
|---|--|
| Passwortwechsel | ☐ Verschlüsselung von Smartphones |
| ☐ Erstellen von Benutzerprofilen | ☐ BIOS-Passwort |
| ☐ Authentifikation mit Benutzername/Passwort | ☐ Automatische Desktopsperre |
| ☐ Regelmäßige Kontrolle von Berechtigungen | ☐ |
| ☐ Zugriffsrechteentzug beim Ausscheiden von | ☐ |
| Personen | |

5. Zugriffskontrolle

Ferner ist die Umsetzung technischer und organisatorischer Maßnahmen zur Sicherstellung der Zugriffskontrolle nötig. Unter Zugriffskontrolle ist die Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben, zu verstehen. Hierfür haben wir die folgenden Maßnahmen ergriffen:

- | | |
|---|---|
| ☐ Erstellung eines Berechtigungskonzepts | ☐ Einsatz einer Antivirensoftware |
| ☐ Verwaltung der Rechte durch einen von Systemadministrator | ☐ Sorgfältige Auswahl und Überprüfung Dienstleistern |
| ☐ Beschränkung der Anzahl der Berechtigungen Administratoren | ☐ Differenzierung zwischen |
| ☐ Passwortrichtlinie inkl. Passwortlänge und von Passwortwechsel | ☐ Einsatz von Benutzerrollen |
| ☐ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten | ☐ Zugriffsrechteentzug beim Ausscheiden Personen |
| ☐ Regelmäßige Überprüfung von Berechtigungen | ☐ Sichere Löschung von Datenträgern |
| ☐ Sperre von Schnittstellen (z.B. USB) | ☐ Sichere Vernichtung von Datenträgern |
| ☐ Verschlüsselung mobiler IT-Systeme | ☐ Trennung von Test- und |
| ☐ Verschlüsselung mobiler Datenträger | ☐ Automatische Sperrmechanismen |
| | ☐ Zwei-Faktor-Authentifizierung |
| | ☐ |
| | ☐ |
| | ☐ |

6. Übertragungskontrolle

Ebenfalls ist die Umsetzung technischer und organisatorischer Maßnahmen zur Sicherstellung der Übertragungskontrolle notwendig. Übertragungskontrolle ist die Gewährleistung, dass überprüft und

festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können, angezeigt.

Hierfür haben wir die folgenden Maßnahmen umgesetzt:

- | | |
|--|--|
| ☐ Nutzung von Signaturverfahren | ☐ Einrichtung von Standleitungen |
| ☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung | ☐ Nutzung von Verschlüsselungs-Technologien |
| ☐ Erstellen einer Übersicht von Abrufverfahren und Übermittlungsvorgängen | ☐ Protokollierung der Zugriffe |
| | ☐ |
| | ☐ |
| | ☐ |

7. Eingabekontrolle

Zudem ist die Umsetzung technischer und organisatorischer Maßnahmen zur Sicherstellung der Eingabekontrolle nötig. Diese ist die Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind. Hierfür wurden folgende Maßnahmen ergriffen:

- | | |
|--|---|
| ☐ Protokollierung der Eingabe, Änderung und Löschung von Daten | ☐ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines |
| ☐ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) | ☐ Berechtigungskonzepts |
| ☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind | ☐ Speicherung von Protokollen der Eingaben, Änderungen und Löschungen |

8. Transportkontrolle

Weiter ist die Umsetzung technischer und organisatorischer Maßnahmen zur Sicherstellung der Transportkontrolle nötig. Unter dieser versteht man die Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit (Art. 32 Abs. 1 lit. b var. 1 DS-GVO) und Integrität (Art. 32 Abs. 1 lit. b var. 2 DS-GVO) der Daten geschützt wird. Zu diesem Zweck wurden folgende Maßnahmen ergriffen:

- | | |
|---|--|
| ☐ Verschlüsselung von E-Mail | ☐ Transport über eine Private Cloud |
|---|--|

- ☐ Erstellen einer Übersicht von ☐ VPN
- ☐ Einrichtung von Standleitungen Abrufverfahren und Übermittlungsvorgängen
- ☐ Beim physischen Transport: sicher Transportbehälter
- ☐ Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und Fahrzeugen

9. Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

Zudem ist die Umsetzung technischer und organisatorischer Maßnahmen zur Sicherstellung der Wiederherstellbarkeit, also einer Gewährleistung, dass eingesetzte Systeme im Störfall wiederhergestellt werden können, nötig. Hierfür haben wir folgende Maßnahmen ergriffen:

- ☐ Erstellung eines Datensicherungskonzepts ☐ Physisch getrennte Speicherung auf gesonderten
 - ☐ Testen der Datenwiederherstellung ☐ Systemen oder Datenträgern
 - ☐ Erstellen eines Notfallvorsorgekonzepts ☐ Regelmäßige Backups
 - ☐ Aufbewahrung von Datensicherungen an ☐
- einem sicheren, ausgelagerten Ort

10. Zuverlässigkeit

Auch ist die Umsetzung technischer und organisatorischer Maßnahmen zur Sicherstellung der Zuverlässigkeit erforderlich. Zuverlässigkeit meint die Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden. Zu diesem Ziel haben wir folgende Maßnahmen umgesetzt:

- ☐ Implementierung von regelmäßigen Patches ☐ Unabhängig voneinander funktionierende
 - IT- und Updates innerhalb unserer Konzepte ☐ Systeme
 - ☐ Geplantes regelmäßiges Auslesen von ☐ Automatisierte Meldung von
 - Fehlfunktionen Fehlerprotokollen ☐ Anti-Viren-Schutz
 - ☐ Bereitstellung redundanter Systeme für ☐
- Notfälle

11. Datenintegrität (Art. 32 Abs. 1 lit. b var. 2 DS-GVO)

Ferner ist die Umsetzung technischer und organisatorischer Maßnahmen zur Sicherstellung der Datenintegrität nötig. Datenintegrität bedeutet die Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können. Hierfür wurden von uns folgende Maßnahmen umgesetzt:

- | | |
|--|---|
| ☐ Regelmäßige Backups des gesamten Systems | ☐ Erstellung eines Datensicherungskonzepts |
| ☐ Speicherung auf mehreren separaten Laufwerken | ☐ |
| | ☐ |

12. Auftragskontrolle

Zudem ist die Umsetzung technischer und organisatorischer Maßnahmen zur Sicherstellung der Auftragskontrolle nötig. Diese meint die Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Hierfür wurden folgende Maßnahmen umgesetzt:

- | | |
|---|--|
| ☐ Schriftliche Vereinbarungen mit den unter Auftragsverarbeitern (Verträge) | ☐ Auswahl jedes Auftragsverarbeiters |
| ☐ Überprüfung der Verpflichtung der Mitarbeiter der Auftragsverarbeiter auf die den Verschwiegenheit | Sorgfaltsgesichtspunkten (insbesondere hinsichtlich der Datensicherheit) |
| ☐ Alle gesetzlich verpflichteten Auftragsverarbeiter haben einen Datenschutzbeauftragten | ☐ Überprüfung und Dokumentation der bei Auftragsverarbeitern getroffenen Sicherheitsmaßnahmen |
| ☐ Sicherstellung der Vernichtung von Daten nach Beendigung des Vertrags | ☐ Laufende Überprüfung aller Auftragsverarbeiter und ihrer Tätigkeiten |
| ☐ Wirksame Kontrollrechte sind mit jedem Auftragsverarbeiter vereinbart | ☐ Vertragsstrafen bei Verstößen |
| | ☐ |
| | ☐ |

13. Verfügbarkeitskontrolle (Art. 32 Abs. 1 lit. b var. 3 DS-GVO)

Auch ist die Umsetzung technischer und organisatorischer Maßnahmen zur Sicherstellung der Verfügbarkeitskontrolle, also einer Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind, nötig. Hierfür haben wir folgende Maßnahmen ergriffen:

- | | |
|---|---|
| ☐ Unterbrechungsfreie Stromversorgung (USV) | ☐ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort |
| ☐ Klimaanlage in den Serverräumen | ☐ Serverräume sind nicht unter sanitären |
| ☐ Geräte zur Überwachung von Temperatur Anlagen platziert und Feuchtigkeit in Serverräumen | ☐ In Hochwassergebieten: Serverräume sind |

- ☐ Schutzsteckdosenleisten in Serverräumen über der Wassergrenze platziert
- ☐ Feuer- und Rauchmelder ☐ Festplattenspiegelung
- ☐ Feuerlöschgeräte in Serverräumen ☐ RAID Systeme
- ☐ Alarmmeldung bei unberechtigtem Zugang ☐
- zu Serverräumen ☐
- ☐ Erstellung eines Datensicherungskonzepts ☐
- ☐ Testen der Datenwiederherstellung
- ☐ Erstellen eines Notfallvorsorgekonzepts

14. Trennbarkeit

Schließlich ist die Umsetzung technischer und organisatorischer Maßnahmen zur Sicherstellung der Trennbarkeit angezeigt. Hierunter versteht sich eine Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können. Zu diesem Zweck haben wir folgende Maßnahmen ergriffen:

- ☐ Physisch getrennte Speicherung auf ☐ Festlegung von Datenbankrechten
- gesonderten Systemen oder Datenträgern ☐ Trennung von Produktivsystem und
- ☐ Logische Trennung (Software) ☐ Testsystemen
- ☐ Erstellung eines Berechtigungskonzepts ☐ Einsatz von mandantenfähigen Systemen
- ☐ Versehen der Datensätze mit ☐
- Zweckattributen / Datenfeldern ☐
- ☐ Sandboxing ☐

15. Pseudonymisierung (Art. 32 Abs. 1 lit. a, 25 Abs. 1 DS-GVO)

Als Pseudonymisierung ist eine Verarbeitung personenbezogener Daten anzusehen, welche ohne Hinzuziehung zusätzlicher Informationen nicht mehr gestattet, eine Information einer spezifischen betroffenen Person zuzuordnen. Im Rahmen der Pseudonymisierung werden die zusätzlichen Informationen gesondert aufbewahrt oder gespeichert und durch geeignete technische und organisatorische Maßnahmen vor unberechtigtem Zugriff bzw. der Entpseudonymisierung geschützt. Zu diesem Zweck haben wir folgende Maßnahmen ergriffen:

- ☐ Pseudonymisierung von Daten in ☐
- Testsystemen ☐
- ☐ Pseudonymisierung von personenbezogenen Daten,
- die nicht mehr im Klartext benötigt werden

- ☐ Interne Richtlinie: Personenbezogene Daten sind im Falle einer Weitergabe oder nach Ablauf von Aufbewahrungsfristen zu anonymisieren oder zu pseudonymisieren

16. Verschlüsselung (Art. 32 Abs. 1 lit. a DS-GVO)

Als Verschlüsselung bezeichnet man die Umwandlung von Klartext in einen schlüsselabhängigen Geheimtext. Nach einer Verschlüsselung kann der Klartext nur unter Verwendung des korrekten Schlüssels wiedergewonnen werden. Folglich ist der Klartext durch die Verschlüsselung vor unberechtigtem Zugriff geschützt. Zu diesem Zweck haben wir folgende Maßnahmen ergriffen:

- | | |
|---|--|
| ☐ Verschlüsselung von Datenträgern | ☐ Verschlüsselung von Webseiten (SSL) |
| ☐ Verschlüsselung von Datenbanken | ☐ |
| ☐ Verschlüsselung von E-Mail | ☐ |
| ☐ Verschlüsselung von Passwörtern | ☐ |

17. Belastbarkeit (Art. 32 Abs. 1 lit. b var. 4 DS-GVO)

Belastbarkeit bedeutet, dass Stabilität hinsichtlich der IT-Systeme gegen Ausfälle oder Angriffe – wie etwa „Denial of Service“-Angriffe – gewährleistet sein muss. Zu diesem Zweck haben wir folgende Maßnahmen ergriffen:

- | | |
|---|---|
| ☐ Einsatz einer unterbrechungsfreien Stromversorgung (USV) | ☐ Einsatz von Load Balancing |
| ☐ Einsatz von Kühlungen in Serverräumen | ☐ |
| ☐ Klimatisierte Serverräume | ☐ |

18. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung technischer und organisatorischer Maßnahmen (Art. 32 Abs. 1 lit. d DS-GVO)

- | | |
|---|---|
| ☐ Benennung eines Datenschutzbeauftragten | ☐ Implementierung eines Prozesses zur |
| ☐ TOM Audit durch den Datenschutzbeauftragten | Durchführung von Datenschutz-Folgenabschätzungen |
| ☐ Regelmäßige Begehungen durch den Datenschutzbeauftragten | ☐ Regelmäßige Überprüfung des Verfahrensverzeichnisses |
| ☐ Regelmäßige Schulungen der | ☐ Regelmäßige Überprüfung des |

Beschäftigten zum Datenschutz

Kategorieverzeichnisses

☐ Mitarbeiterbefragungen zum Datenschutz

☐ Implementierung eines

☐ Überprüfung der Technikgestaltung durch
den Datenschutzbeauftragten

Datenschutzmanagementsystems (DSMS) /

Datenschutzhandbuchs

☐ Gewährleistung von datenschutzfreundlichen Voreinstellungen
durch Einbezug des Datenschutzbeauftragten

Anhang 3

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

- ☐ Audit der TOMs durch die DGD Deutsche Gesellschaft für
Datenschutz GmbH oder
- ☐