Vertrag zur Auftragsverarbeitung (AV-Vertrag)

Fassung vom 02.11.2026 · abrufbar unter https://app.funnelift.com/av-vertrag

zwischen

Merlin Heilemann, handelnd unter „funnelift.com"
Panoramastr. 65, 72070 Tübingen, Deutschland
E-Mail: info@funnelift.com

– im Folgenden **Auftragnehmer** oder **Funnelift** –

und

dem Kunden, der mit Funnelift einen Vertrag über die Nutzung der Software Funnelift geschlossen hat, mit den Angaben aus seinem Kundenkonto

– im Folgenden **Auftraggeber** –

Vorbemerkung: Abschluss dieses Vertrags

Dieser Vertrag wird elektronisch geschlossen (Art. 28 Abs. 9 DSGVO). Der Auftraggeber nimmt ihn bei der Registrierung oder später in seinem Kundenkonto durch Anklicken an. Funnelift speichert Zeitpunkt und Fassung der Annahme; der Auftraggeber kann die jeweils gültige Fassung jederzeit unter https://app.funnelift.com/av-vertrag abrufen, speichern und ausdrucken. Eine Unterschrift ist nicht erforderlich. Bestehende Kunden nehmen diesen Vertrag bei ihrer nächsten Anmeldung an; bis zur Annahme kann er keine Funnels veröffentlichen und keine Änderungen live schalten; bereits veröffentlichte Funnels bleiben online.

1. Einleitung, Geltungsbereich, Definitionen

1.1. Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und Auftragnehmer (im Folgenden „Parteien") im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag im Sinne des Art. 28 der EU-Datenschutz-Grundverordnung (im Folgenden „DSGVO").

1.2. Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen der Auftragnehmer oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten.

1.3. In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der DSGVO zu verstehen. Erklärungen nach diesem Vertrag erfolgen in Textform (z. B. per E-Mail), soweit nicht ausdrücklich etwas anderes bestimmt ist. Mitteilungen des Auftragnehmers an den Auftraggeber gehen an die E-Mail-Adresse des Kundenkontos bzw. an die Inhaber des betroffenen Workspaces; Mitteilungen des Auftraggebers gehen an info@funnelift.com.

1.4. Nicht Gegenstand dieses Vertrags sind Daten, die Funnelift als eigener Verantwortlicher verarbeitet, insbesondere die Daten des Kundenkontos und der Mitglieder des Auftraggebers (Name, E-Mail-Adresse, Anmeldung), Abrechnungsdaten, Support-Anfragen und Protokolle zum Schutz der Plattform. Hierüber informiert die Datenschutzerklärung von Funnelift.

2. Gegenstand und Dauer der Verarbeitung

2.1. Der Auftragnehmer stellt dem Auftraggeber die Software Funnelift bereit. Mit ihr erstellt der Auftraggeber Online-Formulare und mehrseitige Abfragen („Funnels"), veröffentlicht sie unter einer

Adresse von Funnelift oder einer eigenen Domain und empfängt und verwaltet die Angaben der Besucher („Leads"). Der Auftragnehmer übernimmt dabei die Speicherung, Anzeige, Auswertung, Weiterleitung und Löschung der personenbezogenen Daten, die über die Funnels des Auftraggebers erhoben werden (Einzelheiten in Ziffer 3).

Die Verarbeitung beruht auf dem zwischen den Parteien bestehenden Vertrag über die Nutzung der Software Funnelift nach den Allgemeinen Geschäftsbedingungen von Funnelift (im Folgenden „Hauptvertrag"), einschließlich einer kostenlosen Testphase.

2.2. Die Verarbeitung beginnt mit dem Abschluss des Hauptvertrags und endet mit dessen Beendigung. Dieser Vertrag gilt darüber hinaus, solange der Auftragnehmer noch personenbezogene Daten des Auftraggebers verarbeitet (insbesondere bis zur Löschung nach Ziffer 11).

3. Art und Zweck der Datenverarbeitung

3.1. Der Auftragnehmer erbringt digitale Dienstleistungen (Software als Dienst über das Internet). Er speichert die über die Funnels des Auftraggebers erhobenen Daten auf Systemen seiner Unterauftragnehmer (Anlage 2) und greift auf diese Daten nur nach Maßgabe von Ziffer 4.11 zu.

3.2. Die Verarbeitung umfasst insbesondere:

- Erheben der Eingaben von Besuchern über die veröffentlichten Funnels, einschließlich Zwischenständen, wenn der Auftraggeber „Unvollständige Leads" einschaltet;
- Speichern der Leads, hochgeladener Dateien, gebuchter Termine und des Zahlungsstatus;
- Anzeigen, Durchsuchen, Auswerten (Statistik der Aufrufe und Schritte) und Exportieren für den Auftraggeber;
- Versand von E-Mails im Auftrag des Auftraggebers (Benachrichtigung über neue Leads, Bestätigung an den Besucher), soweit der Auftraggeber dies einschaltet;
- Übermitteln von Leads an Empfänger, die der Auftraggeber selbst einrichtet (Webhooks, verbundene Dienste wie E-Mail-Marketing, CRM oder Tabellen, Zahlungsanbieter, Werbenetzwerke), siehe Ziffer 7.10;
- Löschen nach den Einstellungen und Anweisungen des Auftraggebers.

Der Auftraggeber ist ein Unternehmer im Sinne von § 14 BGB, der Funnelift für seine berufliche oder gewerbliche Tätigkeit nutzt (zum Beispiel zur Gewinnung von Kunden, Bewerbern oder Interessenten).

3.3. Die Verarbeitung dient dem Zweck, für den Auftraggeber Anfragen, Bewerbungen, Terminwünsche und sonstige Angaben von Interessenten über Online-Formulare entgegenzunehmen, zu verwalten und an seine eigenen Systeme weiterzugeben. Sie erfolgt im Interesse des Auftraggebers an Kundengewinnung und Kundenbetreuung, Gewinnung von Mitarbeitern, effektivem Kundenmanagement, Vereinfachung seiner Arbeitsabläufe und Messung des Erfolgs seiner Werbung. Welche Angaben ein Funnel im Einzelnen abfragt, bestimmt allein der Auftraggeber.

3.4. Je nach Gestaltung der Funnels durch den Auftraggeber werden folgende Kategorien personenbezogener Daten verarbeitet:

- Kontaktdaten und allgemeine Personendaten (z. B. Name, E-Mail-Adresse, Telefonnummer, Anschrift, Firma);
- Inhalte der Antworten (Auswahl- und Freitextantworten, Bewertungen, Angaben zum Anliegen des Besuchers);
- vom Besucher hochgeladene Dateien (z. B. Fotos, Lebensläufe, Dokumente);
- Inhalte der Funnels, soweit sie personenbezogene Daten enthalten (z. B. Namen, Fotos und Kontaktdaten von Mitarbeitern oder Kunden des Auftraggebers in Texten, Bildern oder

Bewertungen);
- Termindaten (gebuchter Termin);
- Zahlungsdaten: nur Status, Betrag und Kennung der Zahlung beim Zahlungsanbieter des Auftraggebers; Karten- und Kontodaten gibt der Besucher direkt beim Zahlungsanbieter ein, sie erreichen Funnelift nicht;
- Einwilligungsdaten (ob und welcher Einwilligung der Besucher zugestimmt hat, Zeitpunkt);
- Nutzungs- und technische Daten: zufällige Sitzungskennung, aufgerufene Seiten und Schritte, Seitenadresse samt Kampagnen-Parametern (z. B. UTM-Angaben, Klick-Kennungen von Werbenetzwerken), Verweis-Seite, Browserkennung, Geräteart, Sprache, Zeitpunkte;
- IP-Adresse: wird nicht gespeichert, sondern nur kurzzeitig zum Schutz vor Missbrauch und Überlastung verarbeitet sowie, wenn der Auftraggeber die Meta Conversions API einrichtet und der Besucher eingewilligt hat, an Meta übermittelt.

Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO, z. B. Angaben zur Gesundheit, zur ethnischen Herkunft, zu religiösen Überzeugungen oder zum Sexualleben) darf der Auftraggeber nach den AGB von Funnelift (Ziffer 9.9) nicht über die Software verarbeiten. Ihre Verarbeitung ist nicht Gegenstand dieses Vertrags. Erhebt der Auftraggeber solche Daten dennoch, geschieht dies entgegen den AGB und in seiner alleinigen Verantwortung (Ziffern 8.1, 13.4 und 13.6). Personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten (Art. 10 DSGVO, z. B. in Anfragen an Strafverteidiger) darf der Auftraggeber erheben, soweit die Voraussetzungen des Art. 10 DSGVO vorliegen; dafür und für die Information der Besucher ist er allein verantwortlich (Ziffer 8.1). Die Pflichten des Auftragnehmers aus diesem Vertrag, insbesondere zu den technischen und organisatorischen Maßnahmen (Ziffer 5, Anlage 1) und zur Verschwiegenheit (Ziffer 4.13), bleiben unberührt.

3.5. Von der Verarbeitung betroffen sind:

- Besucher der Funnels des Auftraggebers, insbesondere Interessenten, Kunden, Bewerber und Teilnehmer an Umfragen;
- Personen, deren Daten Besucher in einem Funnel angeben (z. B. Ansprechpartner eines Unternehmens);
- Mitarbeiter, Kunden und sonstige Personen, die der Auftraggeber in den Inhalten seiner Funnels nennt oder zeigt.

4. Pflichten des Auftragnehmers

4.1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Er nutzt sie insbesondere nicht für Werbung und nicht zum Training von KI-Modellen.

4.2. Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

4.3. Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.

4.4. Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich in Textform zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.

4.5. Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Derzeit verarbeitet ausschließlich der Auftragnehmer selbst Daten im Auftrag; setzt er weitere Personen ein, sorgt er dafür, dass sie hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.

4.6. Im Zusammenhang mit der beauftragten Verarbeitung unterstützt der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei der Durchführung einer Datenschutz-Folgenabschätzung, soweit dies den Auftragnehmer betrifft. Die dafür erforderlichen Angaben (insbesondere diese Vereinbarung samt Anlagen) stellt er auf Anforderung zur Verfügung.

4.7. Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer, den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist. Dafür stellt der Auftragnehmer in der Software insbesondere bereit: Anzeigen, Bearbeiten, Exportieren und Löschen einzelner Leads, Export aller Leads eines Funnels, Export aller Daten eines Workspaces, Suche und Löschung aller Leads zu einer E-Mail-Adresse („Auskunft und Löschung“) sowie einstellbare Löschfristen je Funnel. Der Auftraggeber nutzt vorrangig diese Funktionen.

4.8. Auskünfte an Dritte oder Betroffene darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.

4.9. Der Auftragnehmer hat nach seiner Prüfung derzeit keinen Datenschutzbeauftragten zu benennen und hat keinen benannt; er überprüft dies mindestens jährlich, insbesondere mit Blick auf den Umfang der Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 37 Abs. 1 lit. c DSGVO). Ansprechpartner für den Datenschutz ist Merlin Heilemann, info@funnelift.com. Wird ein Beauftragter für den Datenschutz benannt, teilt der Auftragnehmer dem Auftraggeber dessen Kontaktdaten unverzüglich mit.

4.10. Die Datenbank und die gespeicherten Dateien liegen in Rechenzentren innerhalb der EU. Einzelne Unterauftragnehmer verarbeiten Daten auch in Drittländern, insbesondere in den USA (Anlage 2). Eine Übermittlung in ein Drittland erfolgt nur unter den in Kapitel V der DSGVO enthaltenen Bedingungen (z. B. Angemessenheitsbeschluss einschließlich EU-US Data Privacy Framework oder Standardvertragsklauseln der EU-Kommission) sowie bei Einhaltung der Bestimmungen dieses Vertrags. Für die in Anlage 2 genannten Unterauftragnehmer erteilt der Auftraggeber hiermit seine Zustimmung; für neue gilt Ziffer 7.

4.11. Zugriff durch den Auftragnehmer auf Inhalte des Auftraggebers: Der Auftragnehmer sieht Funnels und Leads des Auftraggebers grundsätzlich nicht ein. Ein Zugriff erfolgt nur

a. nach Freigabe durch den Auftraggeber über die Funktion „Support-Zugang“ (unter „Team“): Ein Inhaber des Workspaces kann den Zugang für höchstens 7 Tage freigeben und jederzeit vorzeitig beenden. Während der Freigabe hat der Support die Rechte eines Bearbeiters (Funnels ansehen und ändern, Leads ansehen, exportieren und bearbeiten), aber nicht die eines Inhabers. Jeder Tag mit Zugriff wird protokolliert und ist für den Auftraggeber unter „Team“ sichtbar; Exporte und Löschungen stehen zusätzlich im Protokoll des Workspaces;

b. ohne Freigabe nur, soweit dies zur Behebung von Störungen, zur Abwehr von Gefahren für die Sicherheit der Plattform, zur Prüfung gemeldeter rechtswidriger Inhalte nach den AGB (Ziffer 10)

oder aufgrund gesetzlicher Pflichten erforderlich ist, und nur im dafür nötigen Umfang. Zur Prüfung gemeldeter Inhalte sieht der Auftragnehmer nur die Inhalte des Funnels ein, nicht die Leads. Auf Leads greift er ohne Freigabe nur zur Behebung von Störungen, zur Abwehr von Gefahren für die Sicherheit der Plattform oder aufgrund gesetzlicher Pflichten zu und informiert den Auftraggeber darüber unverzüglich, soweit dies gesetzlich zulässig ist. Veröffentlichte Funnels sind ohnehin öffentlich abrufbar.

4.12. KI-Funktionen: Leads und Antworten der Besucher werden nicht an Anbieter von KI-Modellen übermittelt. An den KI-Anbieter (Anlage 2) gehen nur Texte, die der Auftraggeber selbst für eine KI-Funktion eingibt oder auswählt (z. B. Beschreibung seines Angebots, umzuschreibende oder zu übersetzende Texte eines Funnels). Der Auftraggeber gibt in KI-Funktionen keine Angaben von Besuchern oder Leads und keine besonderen Kategorien personenbezogener Daten ein (AGB Ziffer 9.10). Soweit die vom Auftraggeber eingegebenen oder ausgewählten Texte sonstige personenbezogene Daten enthalten (z. B. Namen von Mitarbeitern), verarbeitet der KI-Anbieter sie als Unterauftragnehmer nach Anlage 2.

4.13. Berufsgeheimnisse: Unterliegt der Auftraggeber einer beruflichen Schweigepflicht (insbesondere nach § 203 StGB, § 43a Abs. 2 BRAO, § 57 Abs. 1 StBerG oder als Angehöriger eines Heilberufs), gilt zusätzlich:

a) Der Auftragnehmer ist als mitwirkende Person im Sinne des § 203 Abs. 3 Satz 2 StGB zur Verschwiegenheit über alle fremden Geheimnisse verpflichtet, die ihm bei der Durchführung dieses Vertrags bekannt werden.

b) Der Auftragnehmer ist darüber belehrt, dass er sich nach § 203 Abs. 4 StGB strafbar machen kann, wenn er ein solches Geheimnis unbefugt offenbart; er bestätigt diese Belehrung mit dem Abschluss dieses Vertrags.

c) Der Auftragnehmer verschafft sich von fremden Geheimnissen nur insoweit Kenntnis, wie dies zur Erfüllung dieses Vertrags erforderlich ist (Ziffer 4.11).

d) Der Auftragnehmer setzt weitere Personen und Unterauftragnehmer nur ein, wenn er sie zuvor in Textform zur Verschwiegenheit verpflichtet und über die strafrechtlichen Folgen einer Pflichtverletzung belehrt hat oder sie aufgrund ihrer Vertragsbedingungen einer gleichwertigen Vertraulichkeitspflicht unterliegen.

e) Welche Unterauftragnehmer ihren Sitz außerhalb der EU bzw. des EWR haben oder dort Daten verarbeiten, ergibt sich aus Anlage 2. Der Auftraggeber prüft in eigener Verantwortung, ob der Schutz der Geheimnisse dort vergleichbar gewährleistet ist (§ 43e Abs. 4 BRAO, § 62a Abs. 4 StBerG), und schaltet andernfalls die betreffenden Funktionen für seine Funnels ab (z. B. Antworten in E-Mail-Benachrichtigungen, KI-Funktionen).

f) Diese Ziffer gilt über das Ende dieses Vertrags hinaus.

5. Technische und organisatorische Maßnahmen

5.1. Die in **Anlage 1** beschriebenen Datensicherheitsmaßnahmen (technische und organisatorische Maßnahmen) werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum.

5.2. Die Maßnahmen gemäß vorheriger Ziffer können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat

der Auftragnehmer unverzüglich umzusetzen. Wesentliche Änderungen teilt er dem Auftraggeber mit; die jeweils aktuelle Fassung der Anlage 1 stellt er auf Anforderung bereit.

5.3. Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.

5.4. Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von den Daten anderer Kunden logisch getrennt werden (jeder Datensatz ist einem Workspace zugeordnet, jeder Zugriff wird gegen die Rechte im Workspace geprüft).

5.5. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige Vervielfältigungen, insbesondere Datensicherungen, Zwischenspeicher und Kopien bei der Übertragung, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.

5.6. Die Verarbeitung von Daten im Auftrag außerhalb von Geschäftsräumen (z. B. im Homeoffice oder unterwegs) ist nur mit Geräten zulässig, die die Maßnahmen nach Anlage 1, Ziffer 2 (Zugangskontrolle) erfüllen. Daten im Auftrag werden nicht dauerhaft auf lokalen Geräten oder Datenträgern gespeichert, außer soweit für eine konkrete Aufgabe (z. B. eine vom Auftraggeber gewünschte Datenrettung) vorübergehend erforderlich; danach werden sie gelöscht.

5.7. Der Auftraggeber ist berechtigt, die Erfüllung der Pflichten durch den Auftragnehmer nach Ziffer 8.4 und 8.5 zu kontrollieren.

6. Regelungen zur Berichtigung, Löschung und Einschränkung von Daten

6.1. Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder in der Verarbeitung einschränken. Der Auftraggeber kann dies über die Funktionen der Software selbst tun (Ziffer 4.7).

6.2. Den entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit und auch über die Beendigung dieses Vertrags hinaus Folge leisten.

6.3. Gelöschte Daten sind in der Datensicherung der Datenbank noch bis zu 30 Tage enthalten und werden danach automatisch überschrieben. Eine Wiederherstellung aus der Sicherung erfolgt nur zur Behebung von Störungen oder auf Weisung des Auftraggebers.

7. Unterauftragsverhältnisse

7.1. Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, Unterauftragnehmer einzusetzen (Art. 28 Abs. 2 DSGVO). Die bei Vertragsschluss eingesetzten Unterauftragnehmer sind in **Anlage 2** genannt und gelten als genehmigt. Der Auftragnehmer ist verpflichtet, auf Verlangen des Auftraggebers jederzeit Auskunft über die gegenwärtig und in der Vergangenheit für die Auftragsverarbeitung eingesetzten Subunternehmer zu erteilen. Soweit die Verträge mit Unterauftragnehmern öffentlich zugänglich sind, genügt ein Verweis darauf.

7.2. Der Auftragnehmer informiert den Auftraggeber mindestens 4 Wochen vor dem Einsatz eines neuen oder dem Austausch eines Unterauftragnehmers per E-Mail oder durch einen Hinweis in der Software. Der Auftraggeber kann dem Einsatz innerhalb dieser Frist aus datenschutzrechtlichen Gründen in Textform widersprechen. Können sich die Parteien nicht einigen, kann der Auftraggeber den Hauptvertrag und diesen Vertrag zum Zeitpunkt des Einsatzes kündigen; im Voraus gezahlte Vergütung für die Zeit danach wird anteilig erstattet. Ist ein sofortiger Wechsel zur Abwehr einer

Gefahr für die Sicherheit der Daten oder wegen des Ausfalls eines Unterauftragnehmers nötig, kann die Information nachträglich erfolgen.

7.3. Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind eindeutig voneinander abzugrenzen. Der Auftragnehmer erlegt jedem Subunternehmer vertraglich dieselben Datenschutzpflichten auf, die in diesem Vertrag festgelegt sind, insbesondere hinreichende Garantien für geeignete technische und organisatorische Maßnahmen.

7.4. Weitere Subbeauftragungen durch den Subunternehmer sind nach den Maßgaben der Ziffer 7.1 und 7.3 zulässig.

7.5. Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.

7.6. Die Beauftragung von Subunternehmern, die Verarbeitungen im Auftrag nicht ausschließlich aus dem Gebiet der EU, des EWR oder Staaten mit einem Angemessenheitsbeschluss der EU-Kommission gemäß Art. 45 DSGVO erbringen, ist nur unter Beachtung der in Ziffer 4.10 dieses Vertrags genannten Bedingungen möglich. Sie ist insbesondere nur zulässig, soweit und solange der Subunternehmer angemessene Datenschutzgarantien bietet. Anlage 2 nennt die jeweilige Garantie.

7.7. Der Auftragnehmer überprüft die Einhaltung der Pflichten des Subunternehmers regelmäßig in angemessener Weise. Dazu genügen in der Regel aktuelle Zertifikate, Prüfberichte unabhängiger Stellen (z. B. ISO 27001, SOC 2) oder vergleichbare Nachweise des Subunternehmers. Das Ergebnis ist zu dokumentieren und dem Auftraggeber auf Verlangen vorzulegen.

7.8. Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet hierfür der Auftragnehmer gegenüber dem Auftraggeber nach Maßgabe von Ziffer 13.

7.9. Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise die Inanspruchnahme von Telekommunikationsdienstleistungen oder die Nutzung von Diensten zur Entwicklung der Software ohne Zugriff auf Daten des Auftraggebers, sind nicht erfasst. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

7.10. Keine Unterauftragnehmer von Funnelift sind Empfänger und Dienste, die der Auftraggeber selbst auswählt, einrichtet oder in seine Funnels einbindet, insbesondere: Webhooks, verbundene Dienste (z. B. Google Sheets mit eigenem Dienstkonto, Brevo, Mailchimp, Klaviyo, ActiveCampaign, HubSpot, Pipedrive, Salesforce), sein eigenes Stripe-Konto, Tracking- und Werbedienste (z. B. Meta Pixel und Conversions API, Google Analytics, Google Ads, TikTok, LinkedIn, Pinterest, Snapchat), eigene Skripte, eingebettete Inhalte (z. B. YouTube, Vimeo, Calendly, Cal.com) und Bilder von fremden Servern. Diese Übermittlungen erfolgen auf Weisung des Auftraggebers (Ziffer 10.1). Für die Rechtmäßigkeit, insbesondere für Verträge mit diesen Anbietern, Einwilligungen der Besucher und die Information der Besucher, ist allein der Auftraggeber verantwortlich. Das gilt auch, wenn er für Einbettungen oder Videos die Einstellung „Ohne Klick laden" wählt.

8. Rechte und Pflichten des Auftraggebers

8.1. Der Auftraggeber ist Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO. Er beurteilt die Zulässigkeit der beauftragten Verarbeitung und trägt dafür die Verantwortung; dazu gehören insbesondere eine Rechtsgrundlage für die Erhebung, die Information der Besucher (Datenschutzerklärung und Impressum, die der Auftraggeber in seinen Funnels verlinkt), das Einholen erforderlicher Einwilligungen, die Wahl angemessener Löschfristen und die Wahrung der Rechte betroffener Personen, bei der ihn der Auftragnehmer nach Ziffer 4.7 unterstützt. Der Auftraggeber

stellt sicher, dass er über die Software keine besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) erhebt (AGB Ziffer 9.9). Erhebt er Daten über Straftaten (Art. 10 DSGVO), entscheidet er darüber als Verantwortlicher selbst und trägt die Verantwortung dafür, dass die Voraussetzungen des Art. 10 DSGVO vorliegen, dass er eine gegebenenfalls erforderliche Datenschutz-Folgenabschätzung durchführt und dass die Einstellungen seiner Funnels (z. B. E-Mail-Benachrichtigungen mit Antworten, Tracking, verbundene Dienste) dem Schutzbedarf der Daten entsprechen. Der Auftragnehmer prüft die Inhalte der Funnels nicht auf ihre Rechtmäßigkeit. Die eigenen Pflichten des Auftragnehmers aus diesem Vertrag und aus Art. 28 und 32 DSGVO bleiben unberührt.

8.2. Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich in Textform bestätigen.

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

8.4. Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen, insbesondere die Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen, zu kontrollieren. Vorrangig erfolgt dies durch Einholung von Auskünften und Nachweisen: Der Auftragnehmer beantwortet Fragen des Auftraggebers in Textform, stellt die erforderlichen Unterlagen bereit und verweist auf Zertifikate und Prüfberichte der Unterauftragnehmer. Reicht dies im Einzelfall nicht aus, kann der Auftraggeber die Einhaltung selbst oder durch einen zur Verschwiegenheit verpflichteten, sachkundigen Prüfer, der kein Wettbewerber des Auftragnehmers ist, vor Ort kontrollieren. Die Rechenzentren der Unterauftragnehmer sind hiervon ausgenommen; insoweit gelten deren Nachweise. Daten anderer Kunden dürfen bei einer Kontrolle nicht eingesehen werden. Soweit ein Unterauftragnehmer dem Auftragnehmer selbst Kontrollrechte einräumt, übt der Auftragnehmer sie auf begründetes Verlangen des Auftraggebers für diesen aus und teilt ihm das Ergebnis mit.

8.5. Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen vor Ort nach einer Ankündigung von mindestens 4 Wochen, zu Geschäftszeiten des Auftragnehmers und nicht häufiger als alle 12 Monate statt. Seine eigenen Kosten für Kontrollen trägt jeder Teil selbst.

9. Mitteilungspflichten

9.1. Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis des Auftragnehmers vom relevanten Ereignis an die E-Mail-Adressen der Inhaber des betroffenen Workspaces zu erfolgen. Sie muss, soweit zu diesem Zeitpunkt bekannt (weitere Angaben werden unverzüglich nachgereicht), mindestens folgende Angaben enthalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- den Namen und die Kontaktdaten einer Anlaufstelle für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls

Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

9.2. Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.

9.3. Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.

9.4. Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 32 bis 36 DSGVO im erforderlichen Umfang zu unterstützen, insbesondere bei der Meldung an die Aufsichtsbehörde und der Benachrichtigung betroffener Personen (Art. 33, 34 DSGVO).

10. Weisungen

10.1. Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor. Als Weisungen gelten insbesondere die Einstellungen, die der Auftraggeber oder von ihm berechtigte Mitglieder seines Workspaces in der Software vornehmen (z. B. welche Angaben ein Funnel abfragt, Löschfristen, E-Mail-Benachrichtigungen, Webhooks, verbundene Dienste, Tracking), sowie das Löschen und Exportieren von Daten. Weitere Weisungen erteilt der Auftraggeber in Textform an info@funnelift.com.

10.2. Auftraggeber und Auftragnehmer benennen die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen in **Anlage 3**.

10.3. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen. Änderungen der Inhaber eines Workspaces in der Software gelten als Mitteilung.

10.4. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt oder zu einer Haftung des Auftragnehmers führen kann. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

10.5. Zu einer materiell-rechtlichen Prüfung von Weisungen ist der Auftragnehmer nicht verpflichtet; Ziffer 10.4 bleibt unberührt.

10.6. Weisungen, die über die Funktionen der Software und den vereinbarten Leistungsumfang hinausgehen, behandeln die Parteien als Wunsch nach einer Leistungsänderung. Der Auftragnehmer ist nicht verpflichtet, die Software für einzelne Auftraggeber zu ändern; Ziffer 10.4 bleibt unberührt.

11. Beendigung des Auftrags

11.1. Der Auftraggeber kann seine Daten während der Laufzeit jederzeit selbst exportieren und löschen (Ziffer 4.7), einschließlich des Löschens ganzer Funnels, Workspaces und seines Kontos. Nach Beendigung des Hauptvertrags bleiben die Daten mindestens 30 Tage für den Export abrufbar (Frist für den Datenabruf nach dem Annex der AGB zum Anbieterwechsel). Nach Ablauf dieser Frist löscht der Auftragnehmer alle im Auftrag verarbeiteten Daten des Auftraggebers innerhalb von weiteren 30 Tagen, sofern nicht eine gesetzliche Pflicht zur Speicherung besteht; verlangt der Auftraggeber in Textform eine frühere Löschung, löscht der Auftragnehmer entsprechend früher. Bei Unterauftragnehmern gespeicherte Kopien (z. B. Protokolle des E-Mail-Versands) werden nach den in

Anlage 2 angegebenen Fristen gelöscht. Daten in der Datensicherung werden nach Ziffer 6.3 überschrieben. Auf Verlangen bestätigt der Auftragnehmer die Löschung in Textform.

11.2. Der Auftragnehmer ist verpflichtet, die Löschung auch bei Subunternehmern herbeizuführen. Bei den in Anlage 2 genannten Unterauftragnehmern geschieht dies durch das Löschen in den Systemen, die sie für Funnelift betreiben.

11.3. Der Auftragnehmer hat den Nachweis der ordnungsgemäßen Löschung zu führen und dem Auftraggeber auf Verlangen vorzulegen.

11.4. Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber bei Vertragsende übergeben.

12. Vergütung

Die Vergütung des Auftragnehmers ist abschließend im Hauptvertrag geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieses Vertrags erfolgt nicht.

13. Haftung

13.1. Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, gilt im Außenverhältnis Art. 82 DSGVO.

13.2. Im Innenverhältnis haften die Parteien einander nach dem Anteil ihrer Verantwortung für den Umstand, durch den der Schaden eingetreten ist (Art. 82 Abs. 2 bis 5 DSGVO). Hat eine Partei einer betroffenen Person Schadenersatz geleistet, der über ihren Anteil hinausgeht, kann sie von der anderen Partei den Teil zurückfordern, der deren Anteil an der Verantwortung entspricht (Art. 82 Abs. 5 DSGVO). Für die Beweislast gelten die gesetzlichen Vorschriften.

13.3. Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten oder die von ihm eingesetzten Subdienstleister im Zusammenhang mit der Erbringung der beauftragten vertraglichen Leistung schuldhaft verursachen.

13.4. Die Ziffer 13.3 gilt nicht, soweit der Schaden darauf beruht, dass der Auftragnehmer die beauftragte Dienstleistung korrekt oder eine Weisung des Auftraggebers weisungsgemäß ausgeführt hat (insbesondere Einstellungen nach Ziffer 10.1 und Dienste nach Ziffer 7.10), oder auf der Gestaltung und den Inhalten der Funnels des Auftraggebers, insbesondere auf der Erhebung von Daten ohne ausreichende Rechtsgrundlage oder auf der Erhebung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO) entgegen AGB Ziffer 9.9 (Ziffern 3.4, 8.1). Das gilt nicht, soweit der Auftragnehmer eigene Pflichten aus diesem Vertrag oder der DSGVO verletzt hat, etwa indem er eine offensichtlich rechtswidrige Weisung ohne Hinweis nach Ziffer 10.4 ausgeführt hat. Ziffer 13.1 bleibt unberührt.

13.5. Im Übrigen gelten für die Haftung im Verhältnis der Parteien die Regelungen der AGB von Funnelift (Haftung), soweit dem keine zwingenden gesetzlichen Vorschriften entgegenstehen.

13.6. Der Auftraggeber stellt den Auftragnehmer von Ansprüchen betroffener Personen und sonstiger Dritter frei, soweit diese darauf beruhen, dass a) der Auftragnehmer eine Weisung des Auftraggebers (Ziffer 10.1) befolgt hat, b) die Inhalte der Funnels des Auftraggebers oder die von ihm eingerichteten Dienste nach Ziffer 7.10 gegen Rechtsvorschriften verstoßen c) für eine vom Auftraggeber veranlasste

Erhebung oder Verarbeitung personenbezogener Daten keine ausreichende Rechtsgrundlage bestand oder d) der Auftraggeber entgegen AGB Ziffer 9.9 besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) über die Software verarbeitet hat, und der Auftraggeber dies zu vertreten hat. Der Auftragnehmer stellt den Auftraggeber von Ansprüchen betroffener Personen und sonstiger Dritter frei, soweit diese auf einer vom Auftragnehmer zu vertretenden Verletzung seiner Pflichten aus diesem Vertrag oder der DSGVO beruhen. Hat die freigestellte Partei den Schaden mitverursacht, besteht die Freistellung nur nach dem Anteil der anderen Partei an der Verantwortung (Ziffer 13.2). Die Freistellung umfasst die angemessenen Kosten der Rechtsverteidigung; gegen eine Partei verhängte Geldbußen sind ausgenommen.

13.7. Die in Anspruch genommene Partei informiert die andere Partei unverzüglich in Textform über den Anspruch, erkennt ihn nicht ohne deren Zustimmung an und gibt ihr Gelegenheit, sich an der Abwehr zu beteiligen. Verletzt sie diese Pflichten, entfällt die Freistellung insoweit, als dadurch ein höherer Schaden entstanden ist.

14. Sonderkündigungsrecht

14.1. Der Auftraggeber kann den Hauptvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung"), wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

14.2. Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen, in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.

14.3. Bei unerheblichen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.

15. Sonstiges

15.1. Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrags hinaus vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur Freigabe in Textform durch die andere Partei als vertraulich zu behandeln.

15.2. Sollten Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

15.3. Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform. Der Auftragnehmer kann diesen Vertrag mit Wirkung für die Zukunft ändern, soweit dies wegen einer Änderung der Rechtslage, der Rechtsprechung oder behördlicher Vorgaben erforderlich ist oder die Änderung ausschließlich die Beschreibung der Leistungen und Maßnahmen betrifft, ohne das Schutzniveau für die Daten oder die Rechte des Auftraggebers zu verringern. Er teilt die Änderung mindestens 4 Wochen vor ihrem Wirksamwerden in Textform mit. Widerspricht der Auftraggeber innerhalb dieser Frist in Textform, kann er den Hauptvertrag und diesen Vertrag zum Zeitpunkt des Wirksamwerdens der Änderung kündigen; im Voraus gezahlte Vergütung für die Zeit danach wird anteilig erstattet. Auf das Widerspruchs- und Kündigungsrecht weist der Auftragnehmer in der Mitteilung hin. Der

Auftragnehmer protokolliert, welche Fassung für den Auftraggeber gilt. Für Änderungen der Anlage 2 gilt Ziffer 7.2.

15.4. Die Einrede des Zurückbehaltungsrechts im Sinne des § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten ausgeschlossen.

15.5. Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag gehen in Fragen des Datenschutzes die Regelungen dieses Vertrags vor.

15.6. Es gilt das Recht der Bundesrepublik Deutschland. Es gelten die gesetzlichen Gerichtsstände.

15.7. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Anlage 1 – Technische und organisatorische Maßnahmen

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrechtzuerhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen (Art. 32 DSGVO).

Funnelift betreibt keine eigenen Server. Die Software läuft vollständig auf der Plattform von Cloudflare (Anlage 2). Maßnahmen in den Rechenzentren (Zutritt, Strom, Brandschutz, Hardware) trifft Cloudflare; Funnelift stützt sich dafür auf die Zertifikate und Prüfberichte von Cloudflare (u. a. ISO/IEC 27001, SOC 2 Typ II).

1. Zutrittskontrolle

a. Rechenzentren: Zutrittskontrolle durch Cloudflare und dessen Rechenzentrumspartner (Ausweis- und Zugangssysteme, Videoüberwachung, Sicherheitspersonal), nachgewiesen durch die oben genannten Zertifikate.

b. Funnelift unterhält keine eigenen Serverräume. Arbeitsgeräte, mit denen auf die Verwaltung der Plattform zugegriffen wird, werden in verschlossenen Räumen aufbewahrt und unterwegs nicht unbeaufsichtigt gelassen.

2. Zugangskontrolle

a. Zugang zur Verwaltung der Plattform (Cloudflare-Konto, Quellcode, Zugangsschlüssel) nur für den Auftragnehmer persönlich, mit starkem Passwort und Zwei-Faktor-Anmeldung.

b. Arbeitsgeräte sind mit Passwort und automatischer Bildschirmsperre geschützt und erhalten laufend die Sicherheitsupdates des Betriebssystems. Daten im Auftrag werden nicht auf Arbeitsgeräten gespeichert (Ziffer 5.6 des Vertrags).

c. Anmeldung an der Software: Passwörter mindestens 10 Zeichen, nur als Hash gespeichert (PBKDF2-SHA-256 mit Salz); freiwillige Zwei-Faktor-Anmeldung per Authenticator-App (TOTP) mit Notfall-Codes; Sperre nach wiederholten Fehlversuchen; Links für Einladungen und neue Passwörter nur einmal und befristet gültig; Spamschutz bei der Registrierung (Cloudflare Turnstile) und Bestätigung der E-Mail-Adresse.

d. Sitzungen über signierte, nur für den Server lesbare Cookies (HttpOnly), Abmelden auf anderen Geräten möglich, Passwortänderung beendet andere Sitzungen.

3. Zugriffskontrolle

a. Rollen im Workspace (Betrachter, Bearbeiter, Inhaber) mit abgestuften Rechten; jede Aktion wird auf dem Server gegen die Rolle im Workspace des jeweiligen Funnels geprüft.

b. Zugriff des Auftragnehmers auf Inhalte des Auftraggebers nur nach Ziffer 4.11 des Vertrags (Support-Zugang nur nach Freigabe, befristet auf 7 Tage, protokolliert). Konten mit Betreiber-Rechten können nicht über die Software, sondern nur direkt in der Datenbank vergeben werden.

c. Vom Besucher hochgeladene Dateien sind nicht öffentlich, sondern nur nach Anmeldung und Rechteprüfung abrufbar.

d. Geheime Einstellungen eines Funnels (Webhook-Adressen, Zugangsschlüssel, Empfänger von Benachrichtigungen) werden nicht an Besucher ausgeliefert.

e. Sicherheitsregeln für Skripte (Content Security Policy) im Verwaltungsbereich, der Verwaltungsbereich ist nicht in fremde Seiten einbettbar; von Kunden eingebundene Skripte laufen nicht unter der Adresse des Verwaltungsbereichs.

4. Weitergabekontrolle

a. Alle Verbindungen ausschließlich verschlüsselt (HTTPS mit TLS ab Version 1.2, HSTS), auch für eigene Domains der Kunden (automatische Zertifikate).

b. Zugangsdaten für verbundene Dienste und Zwei-Faktor-Geheimnisse werden zusätzlich verschlüsselt gespeichert (AES-GCM mit 256 Bit).

c. Daten werden laut Cloudflare auf den Datenträgern verschlüsselt gespeichert (Datenbank D1, Dateispeicher R2).

d. Webhooks nur an verschlüsselte Adressen (https), keine Weiterleitungen; Abrufe des Servers nur an öffentliche Adressen.

e. Weitergabe an Dritte nur an die Unterauftragnehmer nach Anlage 2 und an die vom Auftraggeber selbst eingerichteten Empfänger (Ziffer 7.10 des Vertrags); jede Übermittlung an verbundene Dienste wird je Lead protokolliert.

5. Eingabekontrolle

a. Protokoll heikler Aktionen je Workspace (u. a. Exporte, Löschungen, Auskunft und Löschung nach E-Mail, Papierkorb, Verschieben, Mitglieder und Rollen, Support-Zugang, Integrationen), für Inhaber unter „Team" sichtbar, 365 Tage aufbewahrt.

b. Versionsverlauf der Funnels mit letzter bearbeitender Person; Änderungen an abgeschlossenen Leads werden als frühere Antworten aufbewahrt.

c. Protokoll der Tage mit Support-Zugriff, für den Auftraggeber sichtbar.

6. Auftragskontrolle

a. Dieser Vertrag; Weisungen über die Einstellungen der Software und in Textform.

b. Verträge zur Auftragsverarbeitung mit allen Unterauftragnehmern nach Anlage 2; Auswahl nach Eignung ihrer Sicherheitsmaßnahmen und Prüfung anhand ihrer Zertifikate und Berichte mindestens einmal jährlich.

c. Keine Verwendung der Daten für eigene Zwecke, keine Nutzung für Werbung oder zum Training von KI-Modellen.

7. Verfügbarkeitskontrolle

a. Betrieb auf dem verteilten Netz von Cloudflare mit Schutz vor Überlastungsangriffen.

b. Datensicherung der Datenbank laufend durch Cloudflare (Wiederherstellung auf jeden Zeitpunkt der letzten 30 Tage möglich). Hochgeladene Dateien speichert Cloudflare laut Anbieter mehrfach an verschiedenen Orten innerhalb der EU.

c. Begrenzung der Anfragen je Besucher und Funnel (Schutz vor Missbrauch und Spam), Spamschutz beim Absenden.

d. Statusseite mit Prüfung von Datenbank und Datenbankstand, Fehlerprotokoll mit Benachrichtigung des Auftragnehmers per E-Mail, Überwachung der täglichen Wartungsaufgabe.

e. Zustellung von E-Mails und Übermittlungen an verbundene Dienste über eine Warteschlange mit bis zu drei Versuchen.

f. Jede Änderung der Software wird vor der Veröffentlichung automatisch getestet (Prüfung von Code, Darstellung und wichtigen Abläufen im Browser); fehlerhafte Versionen können sofort zurückgenommen werden.

8. Trennungsgebot

a. Logische Trennung der Daten aller Kunden in der Datenbank: Jeder Datensatz gehört zu einem Workspace, jede Abfrage ist auf den Workspace beschränkt; die Trennung wurde durch Zugriffsversuche mit fremden Konten geprüft und wird bei Prüfungen der Software erneut getestet.

b. Entwicklung und Tests ausschließlich mit Beispieldaten in einer getrennten lokalen Umgebung, nicht mit Daten von Kunden.

9. Löschung und Vernichtung

a. Löschfrist für Leads je Funnel durch den Auftraggeber einstellbar; automatische Löschung durch eine tägliche Aufgabe.

b. Gelöschte Funnels liegen 30 Tage im Papierkorb und werden dann mit allen Leads, Dateien und Statistiken endgültig gelöscht; Workspaces und Konten können sofort gelöscht werden.

c. Abgebrochene Datei-Uploads werden nach 2 Tagen gelöscht; Sitzungen, Anmeldeversuche und Einladungen nach festen Fristen.

d. Löschungen in Dateispeicher und bei Domains werden im selben Schritt wie in der Datenbank vorgemerkt und bei Fehlern automatisch nachgeholt.

e. Funnelift nutzt keine eigenen Datenträger für Daten im Auftrag; die Vernichtung ausgemusterter Datenträger in den Rechenzentren erfolgt durch Cloudflare nach anerkannten Verfahren.

10. Fernwartung

Es erfolgt keine Fernwartung durch andere Unternehmen. Wartung und Weiterentwicklung erfolgen ausschließlich durch den Auftragnehmer über verschlüsselte Verbindungen.

11. Belastbarkeit und Wiederherstellung

a. Für Störungen und Datenpannen gibt es einen festgelegten Ablauf (Erkennen, Eindämmen, Bewerten, Informieren, Dokumentieren), einschließlich Benachrichtigung des Auftraggebers nach

Ziffer 9 des Vertrags.

b. Neue Versionen der Software können sofort auf den vorherigen Stand zurückgesetzt werden.

c. Änderungen an der Datenbank sind nur ergänzend, damit ältere Versionen der Software weiterlaufen.

12. Überprüfung und Bewertung

Die Maßnahmen werden bei jeder größeren Änderung der Software und mindestens einmal jährlich überprüft; offene Risiken werden in einer Liste geführt und nach Dringlichkeit behoben.

13. Datensparsame Einstellungen

Für Funnels mit vertraulichen Angaben (z. B. Daten über Straftaten nach Art. 10 DSGVO) stehen dem Auftraggeber in der Software folgende Einstellungen zur Verfügung. Ob er sie nutzt, entscheidet er als Verantwortlicher (Ziffer 8.1 des Vertrags).

a. E-Mail-Benachrichtigungen über neue Leads lassen sich ohne Antworten versenden (Schalter „Antworten in der E-Mail mitschicken“ aus); die E-Mail enthält dann nur einen Link zum Lead in der Software. Den Inhalt von Bestätigungs-E-Mails an Besucher legt der Auftraggeber selbst fest.

b. „Unvollständige Leads“ (Speicherung von Zwischenständen) sind standardmäßig ausgeschaltet und werden nur gespeichert, wenn der Auftraggeber sie einschaltet.

c. Tracking-Pixel erhalten keine Antwortinhalte, sondern nur den Namen der aufgerufenen Seite des Funnels und beim Absenden eine Kennung des Leads; sie laden erst nach Einwilligung des Besuchers. Die Meta Conversions API erhält zusätzlich, nur nach Einwilligung, E-Mail-Adresse, Telefonnummer und Vorname als Prüfsumme (SHA-256). Der Auftraggeber benennt Seiten mit vertraulichen Inhalten neutral oder verzichtet in solchen Funnels auf Tracking.

d. Für Leads lässt sich je Funnel eine Löschfrist einstellen; standardmäßig ist keine Frist gesetzt.

e. Jedes Mitglied kann für sein Konto die Zwei-Faktor-Anmeldung einschalten; der Inhaber kann Mitglieder, die sie nicht nutzen, aus dem Workspace entfernen.

Anlage 2 – Gegenwärtige Unterauftragnehmer

Der Auftragnehmer bedient sich zur Erbringung der Datenverarbeitungen im Auftrag zum Zeitpunkt des Vertragsschlusses der folgenden Unterauftragnehmer:

Unterauftragnehmer	Leistung	Daten	Ort der Verarbeitung und Speicherdauer	Garantie für Drittland
Cloudflare, Inc., 101 Townsend St, San Francisco, CA 94107, USA	Betrieb der gesamten Software: Rechenleistung (Workers), Datenbank (D1), Dateispeicher (R2), Auslieferung der Funnels, eigene Domains, Spamschutz (Turnstile), Schutz vor Überlastung	alle Daten nach Ziffer 3.4	Datenbank (D1) und Dateien (R2): auf die EU beschränkt (Cloudflare-Jurisdiktion „eu“, am 19.10.2026 geprüft). Bearbeitung einzelner Anfragen, Spamschutz und Überlastungsschutz: im weltweiten Netz von Cloudflare, im	EU-US Data Privacy Framework; zusätzlich Standardvertragsklauseln im Vertrag zur Auftragsverarbeitung von Cloudflare

Unterauftragnehmer	Leistung	Daten	Ort der Verarbeitung und Speicherdauer	Garantie für Drittland
	(Rate Limiting), Zwischenspeicher für Bilder, Betriebsprotokolle (Workers Logs)		Rechenzentrum nahe dem Besucher, ohne Speicherung. Zwischenspeicher: nur Bilder aus dem Editor, höchstens 1 Tag. Betriebsprotokolle (Adressen der Aufrufe, Fehlermeldungen): höchstens 7 Tage, Speicherort nicht auf die EU beschränkt. Weitere Cloudflare-Produkte mit Kundendaten (z. B. Queues, KV, Durable Objects) werden nicht genutzt.	
Plus Five Five, Inc. („Resend“), 2261 Market Street #5039, San Francisco, CA 94114, USA	Versand von E-Mails im Auftrag des Auftraggebers (Benachrichtigung über neue Leads, Bestätigung an den Besucher)	Empfängeradresse, Inhalt der E-Mail (je nach Einstellung Antworten des Leads)	Versand über Rechenzentren in der EU (Region eu-west-1, Irland); Speicherung von Inhalt der E-Mails und Versandprotokollen laut Resend in den USA; automatische Löschung bei Resend nach den Aufbewahrungsfristen des Tarifs von Funnelift	EU-US Data Privacy Framework und Standardvertragsklauseln im Vertrag zur Auftragsverarbeitung von Resend
Anthropic Ireland, Limited, 6th Floor, South Bank House, Barrow Street, Dublin 4, D04 TR29, Irland	KI-Funktionen (Funnel mit KI erstellen, Texte umschreiben und übersetzen)	nur Texte, die der Auftraggeber selbst für eine KI-Funktion eingibt; keine Leads (Ziffer 4.12)	Irland; Verarbeitung auch durch Anthropic, PBC in den USA	Standardvertragsklauseln (Übermittlung zwischen Auftragsverarbeitern) im Vertrag zur Auftragsverarbeitung von Anthropic

Nicht als Unterauftragnehmer gelten die Dienste nach Ziffer 7.10 des Vertrags, die der Auftraggeber selbst einrichtet.

Anlage 3 – Weisungsberechtigte Personen

Folgende Personen sind zur Erteilung und Entgegennahme von Weisungen befugt:

1. Weisungserteilung (Auftraggeber)

- die Inhaber des jeweiligen Workspaces (Rolle „Inhaber" in der Software) sowie die Person, die den Hauptvertrag geschlossen hat;
- für Weisungen durch Einstellungen in der Software (Ziffer 10.1) zusätzlich die Mitglieder, denen der Auftraggeber dafür in seinem Workspace die Rolle „Bearbeiter" gibt, im Rahmen dieser Rolle.

2. Weisungsentgegennahme (Auftragnehmer)

- Merlin Heilemann, E-Mail: info@funnelift.com