Vertrag (Vereinbarung) über eine Auftragsverarbeitung nach Art. 28 EU-DSGVO

Datum: _____

Klickpro.de Gerd Breil, Florian Schoel GbR
Am Mühlgraben 5
85435 Erding

(im folgendem Auftragsnehmer genannt)

und

_____

_____

_____

_____

(im folgenden Auftraggeber genannt)

§ 1 Gegenstand und Definitionen

1.1. Dieser Vertrag erfüllt die Anforderungen an die Vereinbarung einer Auftrags(daten)verarbeitung sowohl nach § 11 BDSG-Alt (d.h. die bis zum 25.5.2018 geltende Fassung des BDSG), als auch nach der DSGVO (insbes. § 28 DSGVO). Ab dem 25.05.2018 (nachfolgend bezeichnet als "DSGVO-Stichtag") bestimmt sich die Gültigkeit des Vertrages alleine nach der DSGVO und dann geltenden Datenschutzgesetzen, zu denen insbesondere das BDSG-Neu gehört.

1.2. Im Rahmen dieses Vertrages werden bereits Begrifflichkeiten und Vorschriften der DSGVO verwendet, die jedoch inhaltlich grundsätzlich den Regelungen und Begrifflichkeiten der bis zum DSGVO-Stichtag geltenden Gesetze entsprechen. Sofern Begriffe nachfolgend nicht definiert werden, ist deren Bedeutung bis zum DSGVO-Stichtag im Sinne entsprechend geltender Datenschutzvorschriften zu verstehen.

1.3. Daten - Hierunter sind personenbezogene Daten entspr. § 3 Abs. 1 BDSG-Alt, bzw. Art. 4 Nr. 1 DSGVO zu verstehen. Sofern nicht-personenbezogene/anonyme Daten gemeint sind, werden sie als solche explizit bezeichnet.

1.4. (Datenschutzrechtlich) Verantwortliche Stelle - Der Begriff entspricht der verantwortlichen Stelle im Sinne des § 3 Abs. 7 BDSG-Alt, als auch dem Verantwortlichen im Sinne Art. 4. Nr. 7 DSGVO.

1.5. Verarbeitung - Sofern in diesem Vertrag der Begriff "Datenverarbeitung" oder "Verarbeitung" (von Daten) benutzt wird, wird die Definition der "Verarbeitung" i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

1.6. Auftragsdatenverarbeitung - Hierunter ist die Auftragsdatenverarbeitung gem. § 11 BDSG-Alt sowie die Auftragsverarbeitung gem. Art. 28 DSGVO zu verstehen.

1.7. Bestellung eines Datenschutzbeauftragten - Hierunter ist die Bestellung eines Datenschutzbeauftragten i.A. § 4f BDSG-Alt bzw. dessen Benennung nach Art. 37 DSGVO zu verstehen.

1.8. Technische und organisatorische Maßnahmen - Hierunter sind die nach § 9 BDSG-Alt bzw. die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten zu verstehen.

1.9. Datengeheimnis oder Vertraulichkeits-/Verschwiegenheitsverpflichtung - Hierunter ist das Datengeheimnis gem. § 5 BDSG-Alt sowie eine entsprechende Verpflichtung im Rahmen des Art. 28 Abs. 3 lit. b DSGVO zu verstehen.

1.10. Verfahrensverzeichnisse - Hierunter sind das Verfahrensverzeichnis gem. §§ 4d, 4e BDSG-Alt, bzw. das Verzeichnis von Verarbeitungstätigkeiten nach Art. 32 DSGVO zu verstehen.

1.11. Vorabkontrolle / Datenschutzfolgenabschätzung - Hierunter sind die Vorabkontrolle gem. § 4d Abs. 5 BDSG-Alt, bzw. die Datenschutzfolgenabschätzung nach Art. 35 DSGVO zu verstehen.

1.12. Gegenstand des Auftrags, Datenkategorien, Betroffene, Art, Umfang und Zwecksetzung der Verarbeitung sind entsprechend § 11 Abs. 2 S. 1 Nr. 1 u. 2 BDSG, Art. 28 Abs. 3, 30 Abs. 2 DSGVO bestimmt.

1.13. Verantwortlichkeit und Weisungsrecht bestimmen sich nach § 11 Abs. 2 S. 1 Nr. 4 BDSG-Alt; Art. 28 Abs. 3 lit. a DSGVO.

1.14. Sicherheitskonzept und diesbezügliche Pflichten des Auftragnehmers bestimmen

sich nach § 11 Abs. 2 S. 1 Nr. 9 BDSG-Alt; Art. 28 Abs. 3 u. 32 DSGVO.

1.15. Anfragen Betroffener an den Auftraggeber bestimmen sich nach § 11 Abs. 2 S. 1 Nr.7 BDSG-Alt; Art. 28 Abs. 3 u. 32 DSGVO.
1.16. Informationspflichten und Mitteilungspflichten bei Verstößen bestimmen sich nach § 11 Abs. 2 S. 1 Nr. 8 BDSG-Alt; Art. 28 Abs. 3 lit. f/h, 33 Abs. 2 DSGVO.

1.17. Kontrollbefugnisse und -befugnisse bestimmen sich nach § 11 Abs. 2 S. 1 Nr. 5/7 BDSG-Alt; Art. 28 Abs. 3 lit. h DSGVO.

1.18. Im Fall der Anwendbarkeit des BDSG-Alt bestimmen sich die Informationspflichten bei unrechtmäßiger Kenntniserlangung von Daten nach § 42a BDSG-Alt. Im Fall der Geltung der DSGVO sind Art. 33 und 34 DSGVO einschlägig.

1.19. Für Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber wird auf § 38 BDSG-Alt, Art. 58 DSGVO i.V.m. § 40 BDSG-Neu verwiesen.

1.20. Unterauftragsverhältnisse und Subunternehmer bestimmen sich nach § 11 Abs.2 S.1 Nr. 6 BDSG-Alt; Art. 28 Abs. 2 u. 4 DS-GVO.

1.21. Verarbeitung von Daten in Drittländern bestimmt sich nach §§ 4 b u. 4 c BDSG-Alt; Art. 3 Abs. 2, 44 ff. DSGVO.

1.22. Vertragsbeendigung und Datenlöschung bestimmt sich nach § 11 Abs. 2 S. 1 Nr. 10 BDSG-Alt; Art. 28 Abs. 3 lit. g DSGVO.

1.23. Der Auftragnehmer verarbeitet personenbezogene Daten für den Auftraggeber im Auftrag. Der Auftraggeber hat den Auftragnehmer unter Beachtung seiner gesetzlichen und vertraglichen Sorgfaltspflichten ausgewählt.
Mit Blick auf die hiesige Vereinbarung stellt insbesondere Art. 28 DSGVO bestimmte Anforderungen an eine solche Auftragsverarbeitung.
Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung, deren Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist. Dieser Vertrag wird zur Erfüllung der gesetzlichen Pflichten über Datenverarbeitung im Auftrag geschlossen und verpflichtet den Auftragnehmer nur insoweit, als dies zur Erfüllung der gesetzlichen Pflichten, insbesondere nach § 11 Bundesdatenschutzgesetz, bzw. § 28 ff. Datenschutzgrundverordnung (ab deren Geltung im Mai 2018), erforderlich ist. Darüber hinaus, legt dieser Vertrag dem Auftragnehmer keine weiteren Pflichten auf und begründet insbesondere keine Weisungspflichten des Auftragnehmers. Dies gilt unbeschadet anderweitiger vertraglicher Abreden zwischen den Vertragsparteien.

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst, abhängig vom gebuchten Produkt, Hosting-Leistungen für Webhosting, Management von Servern, Bearbeitung von Webseiten, Bearbeiten von Google AdWords Konto, Bearbeiten von Google Analytics Konto, Bearbeiten von facebook Werbe Konto, Speicherung und Bearbeiten von E-Mails im Zuge von Email Marketing Dienstleistungen, Bereitstellung von Datenbanken und PlugIns, Registrierung von Domains und Skripten, Leistungen in den Bereichen Online- und
E-Mail Marketing, Marketing-Automatisierung, Zurverfügungstellung von Schnittstellen zu anderen Online-Marketing und Automatisierungsprodukten sowie Dienstleistungen, die in einem individuellen Vertrag festgehalten werden.
Der Auftrag umfasst alle notwendigen Arbeiten zur Erbringung dieser Dienstleistungen. Dies umfasst Tätigkeiten, die in den Angeboten / Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortung des für die Verarbeitung Verantwortlichen« im Sinne des Art. 24 EU-DSGVO).

1.24. Die Stelle, die allein oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, ist Verantwortlicher i.S.v. Artikel 4 Ziffer 7 DSGVO. Dies ist der hiesige Auftraggeber.

Die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet, ist der Auftragsverarbeiter i.S.v. Artikel 4 Ziffer 8 DSGVO. Dies ist der hiesige Auftragnehmer.

1.25. Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen, sind personenbezogene Daten i.S.v. Artikel 4 Ziffer 1 DSGVO. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

1.26. Besonders schutzbedürftige personenbezogene Daten sind personenbezogenen Daten gem. Art. 9 DSGVO, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit von Betroffenen hervorgehen, personenbezogene Daten gemäß Artikel 10 DSGVO über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmassregeln sowie genetische Daten gem.

Artikel 4 Ziffer 13 DSGVO, biometrischen Daten gem. Art. 4 Ziffer 14 DSGVO, Gesundheitsdaten gem. Art. 4 Abs. 15 DSGVO sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

1.27. Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüber hinausgehende Verpflichtungen oder Kündigungsrechte ergeben

§ 2 Pflichten des Auftraggebers

2.1. Der Auftraggeber versichert, die Eignung des Auftragnehmers hinsichtlich der Einhaltung der Vorschriften nach dem Bundesdatenschutzgesetz vor der Auftragsvergabe überprüft zu haben Art. 28 Abs. 1 EU-DSGVO).

2.2. Der Auftragnehmer darf Daten nur im Rahmen des Auftrages sowie der Weisungen des Auftraggebers verarbeiten und nur insoweit die Verarbeitung hierzu erforderlich ist. Zweck, Art und Umfang der Datenverarbeitung richten sich ausschließlich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat. Dem Auftraggeber steht das Recht zu, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer in Schriftform oder Textform, d.h. dokumentiert, (Fax/E-Mail) zu erteilen. Die Weisungen können mündlich erfolgen, sofern sie notwendigerweise unverzüglich erteilt werden müssen um die Interessen der Betroffenen oder der Vertragsparteien zu wahren. Im Fall der nicht schriftlichen oder nicht textlichen Weisung müssen die Weisungen unverzüglich in Schriftform oder Textform bestätigt, d.h. dokumentiert, werden.

2.3. Der Auftraggeber ist für die Meldung des Verfahrens an das interne Verfahrensverzeichnis eigenverantwortlich, wobei ihn der Auftragnehmer bei der Erstellung der Unterlagen hinsichtlich der verfahrenstechnischen Angaben unterstützt.

2.4. Der Auftraggeber nimmt alle sich aus dem Bundesdatenschutzgesetz ergebenden Rechte gegenüber dem Betroffenen wahr. Dazu zählen die Berichtigung, Einschränkung der Verarbeitung und Löschung von personenbezogener Daten sowie die Erledigung der Auskunftspflicht an den Betroffenen.

2.5. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter

geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Diese Maßnahmen

schließen unter anderem Folgendes ein: die Pseudonymisierung und Verschlüsselung personenbezogener Daten (Email Verschlüsselung, Datei Verschlüsselung etc), die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen (Zutrittsregelung, Zugangs- und Zugriffsregelung, Datensicherung etc), die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen (Notfallplan, Datensicherungen etc) und ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (regelmäßig Protokollierung mit schriftlicher Dokumentation der Wirksamkeit der Maßnahmen etc.).

2.6. Der Auftraggeber ist für die Sicherheit aller Unterlagen auf dem Transportweg zum Auftragnehmer verantwortlich, wobei der die Art der Sicherheitsmaßnahmen bestimmt.

2.7. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Arbeitsergebnisse festgestellt hat.

2.8. Etwaige Unterauftragsverhältnisse (des Auftragnehmers) sind durch den Auftraggeber schriftlich zu genehmigen (Art. 28 Abs. 2 EU-DSGVO).

2.9. Der Auftraggeber bleibt hinsichtlich bei der Verarbeitung der Daten weisungsbefugt.

§ 3 Pflichten des Auftragnehmers

3.1. Der Auftragnehmer sichert zu, bei der vertragsgemäßen Verarbeitung der personenbezogenen Daten alle in § 2 dieses Vertrages vereinbarten technischen und organisatorischen Sicherheitsmaßnahmen ordnungsgemäß zu erfüllen.

3.2. Der Auftragnehmer berechtigt den Auftraggeber, die Einhaltung der Vorschriften über den Datenschutz und die von ihm getroffenen Weisungen jederzeit zu überprüfen. Die Überprüfung findet nach Absprache statt (Art. 28 Abs. 3 Nr. h) EU-DSGVO). Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Der
Auftragnehmer ist verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen,
soweit seine Daten und Unterlagen betroffen sind. Nicht mehr benötigte Unterlagen mit personenbezogenen Daten und Dateien dürfen erst nach vorheriger Zustimmung durch den

Auftraggeber datenschutzgerecht vernichtet werden. In besonderen, von dem Auftraggeber zu bestimmenden Fällen erfolgt eine Aufbewahrung bzw. Übergabe.

3.3. Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im folgenden Mitarbeiter genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DSGVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

3.4. Der Auftragnehmer verarbeitet die personenbezogenen Daten ausschließlich nach den Weisungen des Auftraggebers. Er verwendet die zur Datenverarbeitung überlassenen Daten nicht für andere Zwecke und bewahrt sie nicht länger auf, als es der Auftraggeber bestimmt hat.

3.5. Der Auftragnehmer versichert, die personenbezogenen Daten nach Weisung durch den Auftraggeber unverzüglich zu berichtigen oder zu löschen.

3.6. Anfallendes Test- und Ausschussmaterial wird vom Auftragnehmer unter Verschluss gehalten, bis es entweder vom Auftragnehmer datenschutzgerecht vernichtet oder an den Auftraggeber zurückgegeben wird. Dasselbe gilt für nicht mehr benötigte Unterlagen mit personenbezogenen Daten aus dieser Auftragsdatenverarbeitung (Art. 28 Abs. 3 Nr. g) EU-DSGVO).

3.7. Aufträge an Unterauftragnehmer werden nur nach schriftlicher Zustimmung durch den Auftraggeber vergeben. Hierunter fallen auch Wartungsarbeiten durch Dritte an den DV-Systemen des Auftragnehmers. Anlass und Art der Arbeiten sind zu protokollieren.

3.8. Der Auftragnehmer unterrichtet den Auftraggeber umgehend bei schwerwiegenden Störungen im Betriebsablauf, bei Verdacht auf Verletzungen gegen Datenschutzbestimmungen oder anderen
Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers, insbesondere bei Ausfall der Sicherheitsmaßnahmen sowie wenn er der Auffassung ist, dass eine Weisung rechtswidrig Ist.

3.9. Bei Störungen im Betriebsablauf, etwa bei Hard- und Softwareaustausch sorgt der Auftragnehmer dafür, dass keine Kundendaten an Dritte weitergegeben werden bzw. dass die Kundendaten vor der Weitergabe zuverlässig gelöscht wurden.

3.10. Die Verarbeitung von Daten des Auftraggebers in außerbetrieblichen Arbeitsstätten ist nur nach Zustimmung des Auftraggebers zulässig und bedarf einer gesonderten Vereinbarung.

3.11. Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme Auftragsdatenverarbeitung erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

§ 4 Kontrolle der Auftragsdatenverarbeitung

4.1. Der Auftragnehmer erklärt sich damit einverstanden, dass die Aufsichtsbehörde, die für die Kontrolle des Datenschutzes beim Auftraggeber zuständig ist, auch bei ihm im begründeten Einzelfall kontrollieren kann. Die Kontrolle wird rechtzeitig angekündigt und findet im Beisein des Auftraggebers statt. In den Fällen, in denen der Auftraggeber mehreren Aufsichtsbehörden zugeordnet ist, muss man sich auf eine bestimmte Aufsichtsbehörde einigen.

4.2. Bei Auftreten von Unregelmäßigkeiten in der Auftragsverarbeitung oder von Verstößen gegen den Datenschutz kann die Überprüfung vor Ort auch unangekündigt erfolgen.

4.3. Der Auftragnehmer sorgt dafür, dass geeignete Unterlagen (etwa nach § 76 BDSG) zur Verfügung stehen, die eine Kontrolle der ordnungsgemäßen Durchführung des Auftrags durch einen sachkundigen Dritten ermöglichen.

§ 5 Steuer, Banken, Factoring

5.1. Die notwendige Weitergabe von Daten an Steuerberater, Finanzamt und Banken (Factoring Banken) bedürfen keiner weiteren Vereinbarung zwischen Auftragnehmer und Auftraggeber.

§ 6 Vertragsdauer

6.1. Die Vertragsdauer wird durch unterschriebene Hauptverträge, Angebote oder Auftragsbestätigungen geregelt.

6.2. Der Auftraggeber ist zu einer außerordentlichen Kündigung des Vertrags berechtigt, wenn der Auftragnehmer trotz schriftlicher Aufforderung die nach § 1 des Vertrages vereinbarte Leistung nicht ordnungsgemäß erbringt oder seine Pflichten nach § 3 dieses Vertrages verletzt.

6.3. Nach der Beendigung des Auftrags gibt der Auftragnehmer alle überlassenen Datenträger an den Auftraggeber zurück und löscht unverzüglich alle bei ihm gespeicherten personenbezogenen Daten aus diesem Auftrag.

§ 7 Vergütung

7.1. Die Vergütung wird durch unterschriebene Hauptverträge, Angebote oder Auftragsbestätigungen geregelt.

7.2. Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise auf eigene Kosten zu kontrollieren.

§ 8 Haftung

Bei fehlerhafter Ausführung der Arbeiten kann der Auftraggeber die kostenlose Berichtigung der Arbeiten verlangen. Der Anspruch auf kostenlose Berichtigung setzt voraus, dass der Auftraggeber die fehlerhaften Arbeiten innerhalb von 3 Monaten nach Auslieferung schriftlich unter Beifügung der für eine Berichtigung notwendigen Unterlagen beanstandet.
Für die Programmerstellung gilt eine Gewährleistungszeit für die Behebung von Programmfehlern von 6 Monaten. Danach auftretende Fehler werden im Rahmen der Wartung zu den üblichen Vergütungssätzen behoben.

§ 9 Schadenersatz

Bei Verstoß gegen die Abmachungen dieses Vertrages, insbesondere gegen die Einhaltung der Maßnahmen zum Datenschutz, wird eine Vertragsstrafe von 15 Prozent des Auftragswertes vereinbart. Den Nachweis hat der Auftraggeber zu erbringen. Etwaige Schadenersatzforderungen von Betroffenen sind gesondert zu regeln.

§ 10 Nichterfüllung der Leistung

10.1. Bei Nichterfüllung der Auftragsleistung durch den Auftragnehmer ist der Auftraggeber berechtigt, soweit er nicht von seinem Kündigungsrecht nach § 6 dieses Vertrages Gebrauch macht, im Benehmen mit dem Auftragnehmer ein anderes Dienstleistungsunternehmen zu beauftragen.
Die dabei entstehenden Mehrkosten gehen zu Lasten des Auftragnehmers.

10.2. Kann der Auftragnehmer die vereinbarte Leistung wegen höherer Gewalt (wie Zerstörung der IT-Technik durch Brand oder eine andere Naturkatastrophe) nicht rechtzeitig erfüllen, so ist er von der Leistung frei. Die Beweislast hierfür obliegt jedoch dem Auftragnehmer. Der Auftraggeber hat in diesem Falle keinen Anspruch auf Schadensersatz. Er hat jedoch das Recht, ein anderes Dienstleistungsunternehmen mit der Auftragsausführung zu beauftragen.

§ 11 Sonstiges

11.1. Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter, etwa durch Pfändung, durch ein Konkurs- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich und vor Eintritt dieser Maßnahmen zu verständigen, damit die Auftraggeberdaten rechtzeitig von den DV-Komponenten des Auftragnehmers genommen werden können.

11.2. Es besteht bei den Vertragsparteien Einigkeit darüber, dass die Allgemeinen Geschäftsbedingungen des Auftragnehmers auf diesen Vertrag keine Anwendung finden.

§ 12 Zustandekommen der Beauftragung

Die Beauftragung kommt durch schriftliche Bestätigung zustande

§ 13 Verarbeitung von Daten in Drittländern (Art. 3 Abs. 2, 44 ff. DSGVO)

13.1. Jeder Verarbeitung der Daten durch den Auftragnehmer findet ausschließlich im Gebiet der Bundesrepublik Deutschland oder in den, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

13.2. Jede Verarbeitung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Dies gilt ebenfalls beim Einsatz von Subunternehmern in Drittländern.

13.3. Sofern eine Verarbeitung von Daten in Drittländern stattfindet, ist der Auftraggeber unbeschadet der Vorgaben der Datenschutzvorschriften und dieses Vertrages auf diese besonders hinzuweisen. Im Hinblick auf Unterauftragsverhältnisse erfolgt der Hinweis im Anhang 2 "Unterauftragsverhältnisse"

§ 14 Gerichtsstand und Schlussbestimmungen

14.1. Änderungen und die Aufhebung des Vertrages und Nebenabreden bedürfen zu ihrer Wirksamkeit der Schriftform.

14.2. Der Auftragnehmer ist verpflichtet, dem Auftraggeber seine aktuelle Anschrift bei jeder Änderung mittels eingeschriebenen Briefes schriftlich mitzuteilen.

14.3. Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit dem Vertragsverhältnis ist der Sitz des Auftraggebers, sofern der Auftragnehmer Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist oder der Auftragnehmer in der Bundesrepublik Deutschland keinen Gerichtsstand hat. Erfüllungsort ist der Sitz des Auftraggebers. Die Rechtsbeziehung zwischen den Vertragsparteien unterliegen ausschließlich dem Recht der Bundesrepublik Deutschland, (welches auch verbindliches Unionsrecht, insbesondere die DSGVO umfasst) - unter Ausschluss von überstaatlichem Recht sowie deutschem, zwischenstaatlichem und überstaatlichem Verweisungsrecht, das nicht selbst auf materielles deutsches Recht verweist und was auch dann keine Anwendung findet, wenn die Vertragspartei ihren Sitz und/oder ihre Wohnanschrift im Ausland hat.

14.4. Sollte eine Bestimmung dieses Vertrags unwirksam oder undurchführbar sein oder werden, so wird die Gültigkeit des Vertrages im Übrigen hiervon nicht berührt. Die Parteien werden sich bemühen, die unwirksame oder undurchführbare Bestimmung durch eine wirksame und durchführbare Regelung zu ersetzen, die der unwirksamen oder undurchführbaren Bestimmung wirtschaftlich so nahe wie möglich kommt. Das gleiche gilt im Falle einer Regelungslücke.

14.5. Ab dem DSGVO-Stichtag am 25.05.2018 können dieser Vertrag, als auch seine Änderungen und Nebenabreden auch auf elektronischen Wege vereinbart/ abgeschlossen werden. Hierbei ist der Zeitpunkt des Vertragsschlusses zu protokollieren und dem Auftraggeber sowie Auftragnehmer nebst dem Vertragstext zugänglich zu machen (z.B. Zusendung per E-Mail oder Zurverfügungstellung im Benutzerbereich einer Onlineplattform).

Ort / Datum	Unterschrift Auftraggeber
Ort / Datum	Unterschrift Klickpro.de (Auftragnehmer)

Anhang 1 - Sicherheitskonzept

Technische und organisatorische Maßnahmen gem. Art. 32 DSGVO
1. Welche Software oder Systeme werden eingesetzt?

Bezeichnung Hersteller Funktionsbeschreibung Bereitstellung Updates / Sicherheit

MacBook Rechner / Mac OS X Apple Büro, Arbeitsmittel
☐ Eigenentwickl. / Individual
☑ Standard- bzw. Kauf-Software
☑ Cloud-Services
☑ Updates
☑ Virenschutz
☑ Firewall

Windows-Rechner Div. Büro, Arbeitsmittel
☐ Eigenentwickl. / Individual

☑ Standard- bzw. Kauf-Software
☑ Cloud-Services
☑ Updates
☑ Virenschutz
☑ Firewall

iOS mobile Software Apple Arbeitsmittel

☐ Eigenentwickl. / Individual
☑ Standard- bzw. Kauf-Software
☑ Cloud-Services
☑ Updates
☑ Virenschutz
☑ Firewall

Android mobile Software Div. Arbeitsmittel ☐ Eigenentwickl. / Individual
☑ Standard- bzw. Kauf-Software
☑ Cloud-Services
☑ Updates
☑ Virenschutz
☑ Firewall

Linux Div. Arbeitsmittel ☐ Eigenentwickl. / Individual
☑ Standard- bzw. Kauf-Software
☑ Cloud-Services
☑ Updates
☑ Virenschutz
☑ Firewall

Im Übrigen wird darauf hingewiesen, dass der Auftragnehmer verpflichtet ist, Software stets auf dem aktuellen Stand zu halten und Virenscanner / Firewalls zu nutzen, sofern gegeben und zum Sicherheitsstandard gehörend.

2. Übermittlung in Drittstaaten
Falls ja: Bitte beschreiben. ☑ nein ☐ ja:
- Der Auftragnehmer übermittelt keine Daten ins Drittland. Falls eine Übermittlung erfolgen sollte, wird diese nur im Rahmen einer Weisung im Rahmen eines Einzelauftrags des Auftraggebers erfolgen.

3. Zutrittskontrolle

Maßnahmen, mit denen Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird:

☑
Zutrittsregelungen für betriebsfremde Personen
- Das Betriebsgebäude des Auftragnehmers ist nicht in unterschiedliche Zutrittsbereiche eingeteilt.
- Der Zutritt zu sämtlichen Datenverarbeitungsanlagen des Auftragnehmers ist Unbefugten vollständig verwehrt.

☐ Alarmanlage
☐ Absicherung von Gebäudeschächten
☐ Automatisches Zugangskontrollsystem
☐ Chipkarten-/Transponder-Schließsystem
☐ Schließsystem mit Codesperre
☑ Manuelles Schließsystem
☐ Biometrische Zugangssperren
☐ Videoüberwachung der Zugänge
☐ Lichtschranken / Bewegungsmelder
☑ Sicherheitsschlösser
☑ Schlüsselregelung (Schlüsselausgabe etc.)
- Die Büroräume sind verschlossen und mit einer elektronischen Zugangskontrolle ausgestattet.
- Nur für die Aufrechterhaltung des Betriebs notwendige Personen sind im Besitz eines Schlüssels.
☐ Personenkontrolle beim Pförtner / Empfang
- Besucher melden sich am Empfang, werden verzeichnet und werden vom Ansprechpartner abgeholt.
- Der Zutritt jeglicher Personen (auch Mitarbeiter) muss durch autorisiertes Personal im Voraus
genehmigt werden und wird durch eine Personenkontrolle überprüft.
☐ Protokollierung der Besucher
☑ Sorgfältige Auswahl von Reinigungspersonal
☐ Sorgfältige Auswahl von Wachpersonal
☐ Tragepflicht von Berechtigungsausweisen
☐ Fenstersicherung (Falls Erdgeschoss oder Einbruchgefahr)

4. Zugangskontrolle

Maßnahmen, mit denen die Nutzung von Datenverarbeitungssystemen durch Unbefugte verhindert wird:
☑ Zuordnung von Benutzerrechten
- Sämtliche Datenverarbeitungsanlagen, die zur Auftragserfüllung notwendig sind, sind passwortgeschützt.
- Die internen Systeme werden per Firewall sowie Benutzername und Passwort und/oder Client-Zertifikate vor unberechtigten Zugriffen geschützt.
- Die Passwörter entsprechen einem technisch sicheren Niveau und sind durch interne Richtlinien geregelt. Die Anmeldung werden protokolliert.
- Mitarbeiter erhalten je nach Tätigkeitsbereich Zugang zu verschiedenen Ebenen des Systems.
- Alle Mitarbeiter werden zentral verwaltet, nach Ausscheiden aus der Firma oder Verlagerung der Tätigkeit werden die Zugänge entsprechend entzogen.

☑ Erstellen von Benutzerprofilen
☑ Passwortvergabe
- Jeder Mitarbeiter vergibt für seinen Arbeitsplatz sein individuelles Passwort, das automatisiert auf seine Sicherheit geprüft wird und niemanden sonst bekannt ist.
☐ Authentifikation mit biometrischen Verfahren
☑ Authentifikation mit Benutzername / Passwort
☑ Begrenzung der Fehlversuche beim Login
☐ Gehäuseverriegelungen
☐ Einsatz von VPN / Verschlüsselungs-Technologie
- Zugriff auf IT-Systeme ist grundsätzlich nur über verschlüsselte und authentifizierte Verbindungen
möglich.
☐ Sperren von externen Schnittstellen (USB etc.)
☐ Einsatz von Intrusion-Detection-Systemen
☐ Verschlüsselung von mobilen Datenträgern
☐ Verschlüsselung von Smartphone-Inhalten
☐ Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)
☑ Einsatz von Anti-Viren-Software
☐ Verschlüsselung von Datenträgern in Laptops / Notebooks
☐ Einsatz einer Hardware-Firewall
☑ Einsatz einer Software-Firewall
☐ Zuordnung von Benutzerprofilen zu IT-Systemen
☐ Regelungen und Sicherheitsmaßnahmen für die Nutzung privater Geräte (z.B. Smartphones)
☐ Verbot mit Genehmigungsvorbehalt und technisch-organisatorische Vorgaben für die Verarbeitung von Daten außerhalb der Betriebsstätte des Auftragnehmers oder von

Subunternehmern (z.B. Telearbeit durch Beschäftigte).

5. Zugriffskontrolle
Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugangsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt, gelesen, kopiert, verändert oder entfernt werden können:

☑ Erstellen eines Berechtigungskonzepts
- Seitens des Auftragnehmers ist der Zugriff auf die IT-Systeme auf solche Personen beschränkt, die die entsprechenden Zugangsberechtigungen haben.

- Ein Berechtigungskonzept (Benutzer- und Administrationsberechtigungen) stellt sicher, dass der Zugriff auf Daten des Systems nur in dem Umfang ermöglicht wird, wie es für die jeweilige Aufgabenerledigung gemäß interner Aufgabenverteilung und Funktionstrennung des Benutzers erforderlich ist. Aus dem Berechtigungskonzept geht hervor, welche Aufgabenträger Administrationsaufgaben (System, Benutzer,
Betrieb, Transport) wahrnehmen und welche Benutzergruppen, welche Aktivitäten im System durchführen können. Verantwortlichkeiten sind geregelt. Dieser Prozessbeinhaltet mindestens einen Beantragungs- und Genehmigungsprozess sowie den Prozess zur Rücknahme von Authentifizierungsmedien und Zugangsberechtigungen. Jeder Zugangsberechtigte darf nur mit den
Anwendungen und innerhalb dieser Anwendungen nur auf die Daten zugreifen, die er zur auftragsgemäßen Bearbeitung des jeweils aktuellen Vorgangs konkret benötigt und die in dem individuellen Berechtigungsprofil eingerichtet sind.
- Systemadministratoren haben Zugriff auf die Verzeichnis-/Dateistruktur der Server; DB-Administratoren haben Zugriff auf die Datenbankserver; Supportmitarbeiter haben lesenden Zugriff auf Kundendaten und Dateien der Accounts. Der Zugriff erfolgt über Benutzername/Passwort. Mitarbeiter können aber nur von Bürorechnern über VPN auf die Anwendung wie auch auf die Server zugreifen. Die Server sind durch eine Firewall geschützt.
- Kunden-/Accountadministratoren haben Zugriff über die Applikation auf Einstellungen der Accounts.
- Die Berechtigungen werden je nach Tätigkeitsbereich vergeben.
☑ Verwaltung der Rechte durch Systemadministrator
☑ Anzahl der Administratoren auf das "Notwendigste" reduziert
☑ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
☑ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
☑ Sichere Aufbewahrung von Datenträgern
☑ Physische Löschung von Datenträgern vor Wiederverwendung

☑ Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
Seite 21 / 27
☑ Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
☑ Protokollierung der Vernichtung
☐ Verschlüsselung von Datenträgern

6. Weitergabekontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.
☐ Verschlüsselung von Daten auf Datenträgern

☐ Festlegung der zur Abgabe von Datenträgern berechtigten Personen
☑ Festlegung des Empfängerkreises
- Daten werden grundsätzlich nicht weitergegeben, außer u.U. an Subunternehmer, sofern diese für die
Ausführung des Auftrags notwendig sind und ihnen zwingende Behördenanfragen zugrunde liegen.
☐ Einrichtungen von Standleitungen bzw. VPN-Tunneln
☐ Weitergabe von Daten in anonymisierter Form
☐ Weitergabe von Daten in pseudonymisierter Form
☑ Verschlüsselung von Websites / Kundenbereich / Uploads.
- Personenbezogene Daten werden grundsätzlich nur verschlüsselt und passwortgeschützt übertragen oder versendet.
- Der Auftragnehmer überträgt von sich aus personenbezogene Daten ausschließlich elektronisch über verschlüsselte Datenverbindungen, so dass sie nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Eine elektronische Übertragung personenbezogener Daten erfolgt ausschließlich im Rahmen des Bestellprozesses, dem Abruf von Kundendaten im Servicefall, innerhalb des
Mahnverfahrens, zur Registrierung von Domains und zur Datensicherung der Kundenumgebungen.
☑ E-Mail-Verschlüsselung
☐ Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
☐ Beim physischen Transport: sichere Transportbehälter/-verpackungen
☐ Kennzeichnung der Datenträger
☐ Bestandsverzeichnis und Bestandskontrolle der Datenträger

- Nicht mehr benötigte oder defekte Datenträger werden durch ein zertifiziertes Unternehmen entsorgt.

7. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wempersonenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind:

☑ Protokollierung der Eingabe, Änderung und Löschung von Daten. Die Verarbeitungstätigkeiten sind durch Server/Software-Logs sowie die internen Anweisungen und Abläufe nachvollziehbar.

☑ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können. Eine derartige Übersicht wird nur erstellt, wenn Art und Umfang der Verarbeitung sich nicht eindeutig aus der Zwecksetzung und dem Funktionsumfang der eingesetzten Software ergeben.

☑ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen). Diese Protokollierung erfolgt,

wenn die verwendete Software die Logins der tätigen Mitarbeiter erfasst. Im Übrigen sind die tätig gewordenen Mitarbeiter anhand internen Anweisungen und Abläufe nachvollziehbar.

☑ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind. Die Aufbewahrung von Formulardaten erfolgt nur, wenn dem eine Weisung von Auftraggebern zugrunde liegt, die Papierform eine rechtliche Relevanz hat, z.B. Nachweis der Einhaltung handschriftlicher Unterschriften bei Schriftformerfordernis.

☑ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts. Mitarbeiter werden nur soweit mit Berechtigungen ausgestattet, als dies für die Erfüllung ihrer Funktionen im Unternehmen sowie Erfüllung zugewiesener Aufgaben erforderlich ist.

☑ Erhebt, verarbeitet oder nutzt ein Auftraggeber im Rahmen des Hostingvertrages personenbezogene Daten, so obliegt es seiner Verantwortung entsprechende Loggingmechnismen für seine Webumgebung zu implementieren.

8. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

☑ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)

☑ Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis / Verschwiegenheit / Vertraulichkeit

☑ Schriftliche Festlegung der Weisungen

☑ Kontrolle der Einhaltung beim Auftragnehmer

☑ Prüfung, ob Auftragnehmer Datenschutzbeauftragten bestellt haben
☑ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

9. Verfügbarkeitskontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:
☑ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
☑ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Es erfolgt ein Backup aller Kundendaten
☐ Zusätzliche Sicherungskopien mit Lagerung an besonders geschützten Orten
☑ Testen von Datenwiederherstellung
☐ Die Verfügbarkeit der Datenverarbeitungssysteme wird permanent überwacht

Auftrag zur Verarbeitung personenbezogener Daten

Anhang 2 - Unterauftragsverhältnisse
(Unterauftragsverhältnisse im Sinne dieses Vertrages, in deren Rahmen Subunternehmer personenbezogene Daten des Auftraggebers verarbeiten, wozu auch die Möglichkeit des Zugriffs oder sonstiger Kenntnisnahme der Daten ausreichend ist.)

Bestehen Unterauftragsverhältnisse?
☐ nein ☑ ja
Auftragsverarbeitungsverträge als Auftraggeber

Buchhaltungssoftware
SuprSale GmbH
Alpenstraße 19
85646 Anzing

Hostingleistungen
GoSuccess GmbH
Alte Holstenstr. 16
21031 Hamburg

E-Mail-Marketing
KLICK-TIPP LIMITED

15 Cambridge Court
210 Shepherd's Bush Road
London W6 7NJ
Vereinigtes Königreich

Factoring
DV Deutsche Verrechnungsstelle GmbH
Wilhelm-Leuschner-Straße 24
60329 Frankfurt am Main