# Vertrag zur Auftragsverarbeitung im Sinne des Art. 28 DSGVO, § 62 BDSG

Regelungen zu Datenschutz und Datensicherheit in Auftragsverhältnissen

zwischen

Firma

Straße

PLZ Ort

– Verantwortlicher –

(nachfolgend „Auftraggeber“ genannt)

und

DREI-D Direktwerbung GmbH & Co. KG

Daimlerstraße 10

25337 Elmshorn

– Auftragsverarbeiter –

(nachfolgend „Auftragnehmer“ genannt)

(beide gemeinsam nachfolgend „Vertragsparteien“ genannt)

# Präambel

1. Zwischen den Vertragsparteien besteht ein Basisvertrag / eine Leistungsvereinbarung über Serviceleistungen.
2. Dieser Vertrag ersetzt mit Inkrafttreten der DSGVO am 25. Mai 2018 einen zwischen den Vertragsparteien möglicherweise bestehenden Auftragsdatenverarbeitungs-vertrag.
3. Unter diesem Vertrag handelt Firma als Verantwortlicher i.S. der DSGVO und der Auftragnehmer als Auftragsverarbeiter im Rahmen einer Auftragsverarbeitung gem. § 28 DSGVO
4. Firma arbeitet nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit der DSGVO und dem BDSG erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet. Der Auftragnehmer bekennt sich zu dieser Verpflichtung.

**Definitionen**

**DSGVO:** Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutzgrundverordnung).

**BDSG:** Bundesdatenschutzgesetz in der jeweils gültigen Fassung, derzeit Bundesdatenschutzgesetz (neu) 2018. Das Gesetz wurde als Teil des Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (DSAnpUG-EU) beschlossen. Diese neue Fassung des BDSG wird am 25. Mai 2018 mit der Datenschutz-Grundverordnung (DS GVO) in Kraft treten und das noch aktuelle Bundesdatenschutzgesetz komplett ersetzen.

**Personenbezogene Daten:** Alle Informationen, die sich auf eine identifizierbare natürliche Person (nachfolgend: **„betroffene Person“** genannt) beziehen. Als identifizierbar ist eine 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.

**Besondere Kategorien von Daten**: Personenbezogene Daten, aus denen die rassische, ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten, Gesundheitsdaten und Daten zum Sexualleben oder der sexuellen Orientierung.

**Datenverarbeitung**: Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

**Auftragsverarbeitung:** Auftragsverarbeitung ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers

Um die Rechte und Pflichten aus dem Auftragsdatenverarbeitungsverhältnis gemäß der gesetzlichen Verpflichtung aus Art. 28 DSGVO zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung.

# 1 Gegenstand des Auftrags, Art und Zweck der Verarbeitung

(1) Der Auftragnehmer verarbeitet für den Auftraggeber personenbezogene Daten im Auftrag des Auftraggebers und nach deren dokumentierten Weisungen (Auftrags-verarbeitung). Dies umfasst alle Datenverarbeitungstätigkeiten, die erforderlich sind, um die Leistungen zu erbringen, die Gegenstand des zwischen den Parteien bestehenden Basisvertrags/Leistungsverzeichnisses sind. Hierbei verarbeitet der Auftragnehmer die personenbezogenen Daten nur, soweit dies zur Erbringung der im Basisvertrag/ in der Leistungsvereinbarung beschriebenen Serviceleistungen notwendig ist.

(2) Die vorliegende Vereinbarung zur Auftragsverarbeitung findet Anwendung auf alle Tätigkeiten, die mit dem Basisvertrag/der Leistungsvereinbarung in Zusammenhang stehen und bei denen der Auftragnehmer, seine Beschäftigten oder durch den Auftragnehmer Beauftragte personenbezogene Daten im Auftrag des Auftraggebers verarbeiten. Eine Verarbeitung personenbezogener Daten des Auftraggebers durch den Auftragnehmer ist darüber hinaus nicht vorgesehen.

(3) Die Verarbeitung der personenbezogenen Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen dokumentierten Weisung des Auftraggebers (Art. 28 Abs. 3 lit. a DSGVO) und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44-49 DSGVO erfüllt sind.

# 2 Art der personenbezogenen Daten, Kategorien betroffener Personen

(1) Art der Daten:

[ ]  Personenstammdaten (Name, Vorname, Straße, PLZ, Ort)

[ ]  Kommunikationsdaten (z.B. Telefon, E-Mail, Fax)

[ ]  Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)

[ ]  Kundenhistorie

[ ]  Vertragsabrechnungs- und Zahlungsdaten

[ ]  Planungs- und Steuerungsdaten

[ ]  Auskunftsangaben von Dritten (z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

[ ]  ……

(2) Kategorien der betroffenen Personen:

[ ]  Kunden (Verbraucher)

[ ]  Kunden (Geschäftskunden)

[ ]  Interessenten

[ ]  Mitarbeiter des Auftraggebers

[ ]  Lieferanten

[ ]  Dienstleister

[ ]  ……..

# 3 Dauer des Auftrages

(1) Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

(2) Der Auftraggeber kann unabhängig von den Regelungen im Hauptvertrag diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer die Erteilung von Auskünften oder den Zutritt des Auftraggebers im Rahmen von Kontrollen vertragswidrig verweigert. Nach der Kündigung darf der Auftragnehmer keine personenbezogenen Daten des Auftraggebers mehr verarbeiten.

# 4 Verantwortlichkeit und Weisungsbefugnis

(1) Der Auftraggeber ist für die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich (Art. 4 Nr. 7 DSGVO). Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Etwas anderes gilt nur in dem in Absatz 2 genannten Umfang.

(2) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers, es sei denn es besteht eine anderweitige Verpflichtung durch Unionsrecht oder dem Recht des Mitgliedsstaates, dem der Auftragnehmer unterliegt. Im Falle einer anderweitigen Verpflichtung teilt der Auftragnehmer dem Auftraggeber vor der Verarbeitung unverzüglich die entsprechenden rechtlichen Anforderungen mit.

(3) Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, informiert er gemäß Art. 28 Abs. 3 S. 3 DSGVO unverzüglich den Auftraggeber. Bis zur Bestätigung oder Änderung der entsprechenden Weisung ist der Auftragnehmer berechtigt, die Durchführung der Weisung auszusetzen.

# 5 Vertraulichkeit

Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die gemäß Art. 28 Abs. 3 S. 2 lit. b DSGVO auf die Vertraulichkeit verpflichtet worden sind und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

# 6 Datensicherheit

(1) Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen zum angemessenen Schutz der personenbezogenen Daten gemäß Art. 28 Abs. 3 lit. c DSGVO in Verbindung mit Art. 32 Abs. 1 DSGVO, um die Sicherheit der Verarbeitung im Auftrag zu gewährleisten. Dazu wird der Auftragnehmer

* die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen,
* die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen, sicherstellen sowie
* ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung unterhalten.

Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

(2) Die Vertragsparteien vereinbaren die in dem **Anlage 1 „Technische und organisatorische Maßnahmen“** zu dieser Vereinbarung niedergelegten konkreten Datensicherheitsmaßnahmen.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber schriftlich mitzuteilen.

# 7 Einbeziehung weiterer Auftragsverarbeiter (Subunternehmer)

(1) Als Subunternehmer im Sinne dieser Regelung gelten vom Auftragnehmer beauftragte Auftragsverarbeiter, deren Dienstleistungen sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht dazu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen und Reinigung in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Subunternehmer nur nach vorheriger ausdrücklicher schriftlicher Zustimmung des Auftraggebers beauftragen.

(3) Werden Subunternehmer eingesetzt, so ist Anlage 2 **„Genehmigte Subunternehmer“** auszufüllen.

# 8 Unterstützung bei der Wahrung von Betroffenenrechten

(1) Der Auftragnehmer ist verpflichtet, den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Wahrung der in Art. 12 bis 22 DSGVO genannten Rechte der betroffenen Personen zu unterstützen (Art. 28 Abs. 3 S. 2 lit. e DSGVO). Insbesondere wird der Auftragnehmer den Auftraggeber darin unterstützen, Ansprüche Betroffener auf Löschung ihrer personenbezogenen Daten gemäß Art. 17 DSGVO zu erfüllen.

(2) Soweit betroffene Personen gegenüber dem Auftraggeber ein Recht auf Datenübertragbarkeit ausüben können, stellt der Aufragnehmer sicher, dass sie die Daten, die sie dem Auftraggeber bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format erhalten können.

(3) Der Auftragnehmer darf personenbezogene Daten nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken (Art. 28 Abs. 3 S. 2 lit. g DSGVO). Auskünfte an Dritte oder den betroffenen Personen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

(4) Soweit eine betroffene Person sich unmittelbar an den Auftragnehmer wendet, um ihre Rechte gemäß Art. 12 bis 22 DSGVO geltend zu machen, wird der Auftragnehmer das Ersuchen unverzüglich an den Auftraggeber weiterleiten.

# 9 Unterstützung bei Dokumentations- und Meldepflichten

(1) Ist der Auftragnehmer nach Art. 37 DSGVO, § 37 BDSG-neu gesetzlich dazu verpflichtet, einen Datenschutzbeauftragten zu benennen, teilt der Auftragnehmer dem Auftraggeber die Kontaktdaten des Datenschutzbeauftragten zum Zweck der direkten Kontaktaufnahme mit. Ein Wechsel des Datenschutzbeauftragten ist bei dem Auftraggeber unverzüglich anzuzeigen.

Als Datenschutzbeauftragter ist beim Auftragnehmer

Dipl.-Jur.(FH) Nicolas Reinheimer

Externer Datenschutzbeauftragter

FKC Management-System-Beratung GmbH | 20097 Hamburg | Frankenstr. 7

N.Reinheimer@fkc-gmbh.de
bestellt.

# 10 Beendigung des Auftrages

(1) Nach Abschluss der Erbringung der Verarbeitungsleistungen hat der Auftragnehmer alle personenbezogenen Daten nach Wahl des Auftraggebers entweder zu löschen oder zurückzugeben, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

(2) Der Auftragnehmer weist unaufgefordert dem Auftraggeber in Textform mit Datumsangabe nach, dass er sämtliche Datenträger sowie sonstigen Unterlagen an den Auftraggeber herausgegeben oder datenschutzkonform vernichtet oder gelöscht und somit keine Daten des Auftraggebers zurückbehalten hat.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

# 11 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber ist berechtigt, vor Beginn der Verarbeitungsleistungen und währenddessen regelmäßig die technischen und organisatorischen Maßnahmen sowie die Einhaltung dieser Vereinbarung und datenschutzrechtlicher Vorgaben zu kontrollieren. Dazu kann der Auftraggeber oder ein beauftragter Prüfer die Datenverarbeitungsanlagen und die Datenverarbeitungsprogramme des Auftragnehmers inspizieren.

(2) Der Auftragnehmer ist verpflichtet, dem Auftraggeber zu den üblichen Geschäftszeiten Zutritt zu den Räumlichkeiten zu gewähren, in denen die Daten des Auftraggebers physisch oder elektronisch verarbeitet werden. Der Auftraggeber stimmt die Durchführung der Inspektionen mit dem Auftragnehmer so ab, dass der Betriebsablauf beim Auftragnehmer so wenig wie möglich beeinträchtigt wird.

(3) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der technischen und organisatorischen Maßnahmen sowie der Einhaltung dieser Vereinbarung und datenschutzrechtlicher Vorgaben zur Verfügung. Zu diesen Informationen gehören insbesondere aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, externe Sachverständige, IT-Sicherheits- oder Datenschutzauditoren) und geeignete Zertifizierung (z.B. nach BSI-Grundschutz). Der Auftragnehmer erteilt dem Auftraggeber unverzüglich konkrete Auskunft im Einzelfall.

# 12 Haftung

(1) Auftraggeber und Auftragnehmer haften im Außenverhältnis nach Art. 82 Abs. 1 DSGVO für materielle und immaterielle Schäden, die eine Person wegen eines Verstoßes gegen die DSGVO erleidet. Sind sowohl der Auftraggeber als auch der Auftragnehmer für einen solchen Schaden gemäß Art. 82 Abs. 2 DSGVO verantwortlich, haften die Parteien im Innenverhältnis für diesen Schaden entsprechend ihres Anteils an der Verantwortung. Nimmt eine Person in einem solchen Fall eine Partei ganz oder überwiegend auf Schadensersatz in Anspruch, so kann diese von der jeweils anderen Partei Freistellung oder Schadloshaltung verlangen, soweit es ihrem Anteil an der Verantwortung entspricht.

(2) Der Auftragnehmer haftet dem Verantwortlichen gegenüber entsprechend auch für die Einhaltung datenschutzrechtlicher Vorgaben durch die Subunternehmer, die er zur Erfüllung seiner Aufgaben einsetzt. Das Verschulden von Subunternehmern ist dem Auftragnehmer wie eigenes Verschulden zuzurechnen.

(3) Der Auftragnehmer unterstützt den Auftraggeber mit allen ihm zur Verfügung stehenden Informationen, wenn der Auftraggeber einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist.

# 13 Schlussbestimmungen

(1) Überlassene Datenträger und Datensätze verbleiben im Eigentum des Auftraggebers.

(2) Sollten einzelne oder mehrere Regelungen dieser Vereinbarung unwirksam sein, so wird die Wirksamkeit der übrigen Vereinbarung hiervon nicht berührt. Für den Fall der Unwirksamkeit einzelner oder mehrere Regelungen werden die Vertragsparteien die unwirksame Regelung unverzüglich durch eine solche Regelung ersetzen, die der unwirksamen Regelung wirtschaftlich und datenschutzrechtlich am ehesten entspricht.

(3) Im Falle eines Widerspruchs zwischen dem Hauptvertrag und dieser Vereinbarung geht diese Vereinbarung vor, soweit der Widerspruch die Verarbeitung personenbezogener Daten betrifft.

(4) Alle Leistungen des Auftragnehmers in Zusammenhang mit der Erfüllung seiner Pflichten aus dieser Vereinbarung sind mit der Vergütung aus dem Hauptvertrag abgegolten.

(5) Die folgenden Anhänge sind Bestandteil dieser Vereinbarung:

* Anlage 1 „Technische und organisatorische Maßnahmen“
* Anlage 2 „Genehmigte Subunternehmer“

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ort, Datum: |   |  | Ort, Datum: |  |
|  |  |  |
| **Stempel, Unterschrift Auftraggeber** |  | **Stempel, Unterschrift Auftragnehmer** |