Auftragsverarbeitungsvertrag

zwischen

_____
_____
_____
_____

(i. f. Auftraggeber)

und

Terminmaschine
Finanzmedia
Elmar Spitz
HRCOMTEC GmbH
Karl Marx Str.16 68199 Mannheim
Handelsregister: HRB 737180
Registergericht: Mannheim
Vertreten durch GF Elmar Spitz

(i. f. Auftragnehmer)

Inhalt

1 Gegenstand und Dauer der Vereinbarung[1]

a) Der Auftrag umfasst Folgendes:

Der Gegenstand des Auftrags und die konkrete Beschreibung der vertraglich vereinbarten Leistungen:

sind dem Hauptvertrag[2] unter

X oder dem **Anhang A**

zu entnehmen.

b) Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 auf Grundlage dieses Vertrages.

c) Die vertraglich vereinbarte Leistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der vertraglich vereinbaren Leistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

d) **Dauer des Auftrags**

Die Dauer des Vertrags

beginnt am und endet am

wird auf unbestimmte Zeit geschlossen. Kündigungsfrist ist

X entspricht der Laufzeit des Hauptvertrages[2]

e) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

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

Verweis auf

	Hauptvertrag[2]	X	**Anhang A**
	Leistungsverzeichnis		weitere, als Anlage beigefügte Unterlagen

3 Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

a) Für die Beurteilung der Zulässigkeit der Verarbeitung nach Art. 6 Abs. 1 sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche

[1] Vorschriften mit der Vorbezeichnung Art. sind solche der EU-Datenschutzgrundverordnung (DSGVO)

[2] Als Hauptvertrag sind definiert Rahmen-, Werk-, Dienstleistungs- oder Einzelvertrag

Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

b) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einer dokumentierten elektronischen Form festzulegen.

c) Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einer dokumentierten elektronischen Form zu bestätigen.

d) Der Auftraggeber ist berechtigt, sich wie unter Nr. 5 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen. Jede der Vertragsparteien trägt die hierfür bei ihnen anfallenden Kosten selbst.

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

f) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4 Ansprechpartner des Auftraggebers und des Auftragnehmers

a) Ansprechpartner des Auftraggebers sind:

Der/ die Unterzeichner*in

b) Ansprechpartner beim Auftragnehmer sind:

Elmar Spitz Karl Marx Str. 16, 68199 Mannheim

elmar.spitz@terminmaschine.de 0621 - 81 91 089 0

c) Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen.

5 Pflichten des Auftragnehmers

a) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftraggeber unterliegt, verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftraggeber dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 a).

b) Alle Weisungen sind für Geltungsdauer des Vertrages und anschließend noch für drei volle Kalenderjahre aufzubewahren.

c) Der Auftragnehmer sichert zu, dass er keiner gesetzlichen Verpflichtung eines Landes unterliegt, welche die Preisgabe von personenbezogenen Daten ohne richterlichen Durchsuchungsbefehl fordert. Wird ein solcher richterlicher Beschluss vorgelegt, ist der Auftraggeber unverzüglich darüber zu informieren. Sollte eine Behörde außerhalb der Europäischen Union oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum Zugriff auf die Daten des Auftraggebers verlangen oder erhalten, begründet dies seitens des Auftraggebers ein außerordentliches Kündigungsrecht für diese Auftragsverarbeitung.

d) Soweit Prüfungen von Aufsichtsbehörden beim Auftragnehmer durchgeführt werden, verpflichtet sich dieser, umgehend die Tatsache der Prüfung wie auch das Ergebnis im Hinblick auf das Auftragsverhältnis dem Auftraggeber bekannt zu geben. Dies gilt auch, soweit eine zuständige Behörde nach Art. 58 Abs. 1 beim Auftragnehmer ermittelt.

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

f) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

g) Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang werden dokumentiert.

h) Der Auftragnehmer hat über die gesamte Laufzeit des Vertrags für den Auftraggeber insbesondere folgende Überprüfungen in seinem Bereich durchzuführen (Art.32 Abs. 1):

Das Ergebnis der Kontrollen ist zu dokumentieren.

i) Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 e, f). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an die in Ziff. 4 genannte weisungsberechtigte Person beim Auftraggeber weiterzuleiten.

j) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

k) Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

l) Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder betroffenen Personen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

m) Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 h). Jede der Vertragsparteien trägt die hierfür bei ihnen anfallenden Kosten selbst.

n) Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt. Hierzu wird vereinbart, dass mindestens

   - ein Ansprechpartner zur Verfügung steht
   - Systemeinsicht ermöglicht wird
   - Zugriff auf ergänzende Unterlagen gewährt wird
   - falls erforderlich ein Arbeitsplatz beim Auftragnehmer zur Verfügung gestellt wird.

o) Die Verarbeitung von Daten außerhalb der Geschäftsräume des Auftragnehmers (Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) ist nur mit Zustimmung des Auftraggebers gestattet. In diesem Fall werden die Vorgaben aus **Anhang B** zum Vertragsgegenstand. Die Zustimmung des Auftraggebers, der Umfang der Zugriffsberechtigung und die fallorientierten Sicherungsmaßnahmen sind zu dokumentieren.

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

X	Bankgeheimnis	X	Fernmeldegeheimnis
	Sozialgeheimnis		Berufsgeheimnisse nach § 203 StGB (bei Einzelvertrag s. **Anhang C**)
	sonstige Gesetze:		

q) Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

r) Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 b und Art. 29). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

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

Susanne Mappes Karl Marx Str. 16 Mannheim datenschutz@terminmaschine.de
Externer Datenschutzbeauftragter:
IITR GmbH Eschenrieder Str. 62c, 82194 Gröbenzell
bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

s) Hat dieser Vertrag die Wartung/Prüfung automatisierter Verfahren oder von Datenverarbeitungsanlagen zum Inhalt werden die Vorgaben aus **Anhang D** zum Vertragsgegenstand.

t) Der Auftragnehmer verpflichtet sich, den Auftraggeber über den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 und den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 unverzüglich zu informieren.

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

Der Auftragnehmer teilt dem Auftraggeber unverzüglich nach Kenntnisnahme Verstöße

- des Auftragnehmers, der bei ihm beschäftigten Personen oder bei Subunternehmern gegen datenschutzrechtliche Bestimmungen
- gegen die im Auftrag getroffenen Festlegungen mit.

Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 f). Meldungen nach Art. 33 oder 34 für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung nach Ziff. 4 dieses Vertrages durchführen.

7 Unterauftragsverhältnisse mit Subunternehmern

(Art. 28 Abs. 3 Satz 2 d)

a) Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet (Art. 28 Abs. 2), welche auf einem der o. g. Kommunikationswege (Ziff. 4) in Textform erfolgen muss. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

b) Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Leistungen zu verstehen, die der Auftragnehmer durch Dritte als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z. B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Informations-/Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

c) Eine Beauftragung von Subunternehmern unter den Voraussetzungen von Ziff. 7 a dieses Vertrages in Drittstaaten darf nur erfolgen, wenn zusätzlich die besonderen Voraussetzungen der Art. 44 ff. erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

d) Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen. Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9).

e) Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 bezüglich seiner Beschäftigten erfüllt hat.

f) Der Auftragnehmer hat die Einhaltung der Pflichten des/der Subunternehmer(s) wie folgt zu überprüfen:

Durch Überprüfung der Zertifizierung der technischen Anlagen der Subunternehmer Es werden ausschließlich von STRATO AG Pascalstraße 10 10587 Berlin und 1&1 Ionos SE Elgendorfer Str. 57 56410 Montabaur betriebene Datenverarbeitungsanlagen verwendet

g) Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen.

h) Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

i) Zurzeit sind für den Auftragnehmer die in **Anhang F** mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

j) Die Erweiterung des Auftragsumfangs bei bestehenden Subunternehmern steht unter dem Vorbehalt der Genehmigung des Auftraggebers.

k) Widerspricht der Auftraggeber der Erweiterung des Auftragsumfangs bei bestehenden Subunternehmen oder der Hinzuziehung weiterer, bisher nicht involvierter Subunternehmer und ist dadurch dem Auftragnehmer die Erfüllung des Auftrags nicht mehr möglich, erlischt dieser Vertrag.

8 Technische und organisatorische Maßnahmen

(Art. 28 Abs. 3 Satz 2 c)

a) Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

b) Die Daten haben einen hohen Schutzbedarf. Für die auftragsgemäße Verarbeitung personenbezogener Daten wird folgende Methodik zur Risikobewertung verwendet, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten für die betroffenen Personen berücksichtigt:

   Risikobewertung erfolgte auf Basis der Informationsklassifizierung und der daraus erforderlichen Maßnahmen und Sicherheitsmechanismen. Die in Anhang E beschriebnen Vorkehrungen und Festlegungen tragen dem Schutzbedarf ausreichend Rechnung

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

d) Diese Maßnahmen müssen im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung (Stand der Technik) angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

e) Folgende Möglichkeiten für den Nachweis durch Zertifizierung bestehen:

   Die Bewertung des Risikos samt der Auswahl der geeigneten technischen und organisatorischen Maßnahmen des Auftragnehmers wurden am durch folgende unabhängige externe Stellen auditiert/zertifiziert gemäß den Regelungen nach Art. 42:

   Diese vollständigen Prüfunterlagen und Auditberichte können vom Auftraggeber jederzeit eingesehen werden.

   X Der Auftragnehmer hat regelmäßig, mindestens aber alle zwei Jahre oder bei wesentlichen Änderungen der technischen und organisatorischen Maßnahmen, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 d).

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

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

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

9 Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags

(Art. 28 Abs. 3 Satz 2 g)

a) Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen,

  dem Auftraggeber auszuhändigen.

  X wie folgt datenschutzgerecht zu löschen bzw. zu vernichten/vernichten zu lassen:
  gemäß den gesetzlichen Vorgaben

b) Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

c) Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

10 Haftung

Hierzu wird auf Art. 82 verwiesen.

11 Sonstiges

a) Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

b) Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

c) Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

d) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

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

f) Die Regelungen dieser Vereinbarung nebst Anlagen haben Vorrang gegenüber etwaig entgegenstehenden oder abweichenden Regelungen aus anderen Vertragsbestandteilen des Vertragswerkes (wie dem Hauptvertrag und dessen Anlagen).

12 Anhänge

Folgende Dokumente sind Gegenstand dieser Vereinbarung zur Auftragsverarbeitung:

X Anhang A → Art und Zweck der Verarbeitung, ...
X Anhang B → Mindestanforderungen bei mobilem Arbeiten
X Anhang C → Geheimnisschutz nach § 203 StGB
Anhang D → Mindestanforderungen bei Fernzugriff …..
X Anhang E → Technische- u. organisatorische Maßnahmen …..
X Anhang F → Subunternehmer

Mannheim, Februar 2020	
	Ort, Datum
Unterschrift Auftragnehmer	Unterschrift Auftraggeber
Elmar Spitz	
in Druckbuchstaben	in Druckbuchstaben

Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorien der betroffenen Personen

Anhang A

1. Vertragsinformationen

Vertragsbezeichnung und Vertragsdatum des Hauptvertrages[1]

2. Art und Zweck der Verarbeitung

Ergeben sich die Art und der Zweck der Verarbeitung aus dem Hauptvertrag, ist hier nur auf die entsprechenden Vertragsbestimmungen zu verweisen.

Konkrete Darstellung der Art der Verarbeitung:

Terminmaschine stellt dem Auftraggeber eine Webanwendung zur Verfügung, die Terminmaschine genannt wird.

Personenbezogene Daten werden zu folgenden Zwecken erhoben und / oder verarbeitet:

Terminmaschine erhebt, verarbeitet und speichert personenbezogenen Daten, um die Nutzung der von Terminmaschine angebotenen Dienste zu ermöglichen und zu optimieren. Terminmaschine nutzt die erhobenen Daten zur Vertragserfüllung und für Werbezwecke.

3. Art der personenbezogenen Daten

Folgende Datenarten sind betroffen:

E-Mail-Adresse
- T2: Browser- und Systemdaten
- T3: IP-Adresse
- T4: Sprache
- T5: Zeitzone
- T6: Sämtliche Daten, die vom Email/Videolink-Empfänger auf eigene Veranlassung im Kundenkontaktformular eingegeben werden
- T7: Ggf. weitere Daten, die durch den Auftragsgeber von einem Videolink-Empfänger abgefragt werden, wie beispielsweise der Vorname, der Nachname, die Telefonnummer oder eine Kundennummer
- T8: Anonymisierte Nutzungsdaten, die sich aus der Nutzung der Terminmaschine ergeben (z.B. Video-Link Aufrufzahlen)
- T9: Zeitinformationen der Videoübertragung, (vom Auftraggeber abschaltbar, je nach DSGVO Kontakterklärung des Email/Videolink-Empfängers)
- T10: Opt-In, Opt-Out-Status des Kontaktformulars und der Linkversendung des Email/Videolink-Empfängers mit Zeitinformation

4. Kategorien der betroffenen Personen

Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorien der betroffenen Personen

Ergibt sich der Kreis der betroffenen Personen bereits aus dem Hauptvertrag, ist hier nur auf die entsprechenden Vertragsbestimmungen zu verweisen.

Email/Videolink-Empfänger sind Personen, die vom Auftraggeber Email/Videolinks zugesandt bekommen.

Mindestanforderungen bei mobilem Arbeiten[1]

Anhang B

Abkürzungen:

AV	= Auftragsverarbeitung	BYOD	= Bring your own Device
DSGVO	= Datenschutzgrundverordnung		

Lässt der Auftragnehmer im Rahmen einer AV Tätigkeiten im Rahmen des mobilen Arbeitens durchführen, müssen die nachfolgend aufgeführten Vorgaben erfüllt sein. Die technische Umsetzung dieser Vorgaben kann im Einzelnen abweichen, muss aber den geforderten Schutzzweck der Maßnahme voll erfüllen.

1. Garantien des Auftragnehmers

Die nachfolgenden Vorgaben sind durch den Auftragnehmer sicherzustellen und sind Grundlage des AV-Vertrages:

1.1. Einhaltung aller technisch-/organisatorischer Maßnahmen aus dem AV-Vertrag Anhang E

1.2. Zusicherung, dass auf den mobilen Arbeitsplätzen die nachfolgenden Maßgaben eingehalten werden

1.2.1. Trennung vom Privatbereich sowohl räumlich als auch technisch

- Abschließbares Büro bzw. alle Dokumente und die DV-Hardware müssen zugriffsgeschützt (z. B. abschließbarer, nicht allgemein zugänglicher Schrank) aufbewahrt werden
- Physische Trennung zwischen beruflichem und privatem (Internet)-Anschluss - alternativ äquivalente Schutzmaßnahmen entsprechend den Stand der Technik
- Die betrieblich gestellte DV-Hardware ist nur für die berufliche Nutzung zu verwenden
- Sonderformen wie z. B. BYOD oder auch Virtualisierung auf BYOD-Geräten müssen dem Auftraggeber zuvor explizit technisch dargelegt und von diesem genehmigt werden
- Berufliche Mails dürfen nicht auf private Postfächer umgeleitet werden

1.2.2. Verbindung nur über gesicherte Kommunikationswege (nach Stand der Technik)

1.2.3. Dateiverschlüsselung bei mobilen Geräten und Datenspeichern (z. B. Festplatten, USB-Sticks, ...) nach dem jeweiligen Stand der Technik

1.2.4. Einsatz einer Datenverschlüsselung bei Übermittlung und Speicherung gemäß dem jeweiligen Stand der Technik

1.2.5. Dokumentation des Versands/der Mitnahme aller Dokumente auf mobile Arbeitsplätze

1.2.6. Der Zugriff (auch via Virtualisierung) von einem mobilen Arbeitsplatz in unsicheren Ländern der EU[2] oder Drittländern ist nur nach vorheriger Zustimmung durch den Auftraggeber erlaubt

[1] hierunter sind auch z. B. Heim-/Telearbeitsplätze zu verstehen

[2] als unsichere Länder in der EU werden derzeit angesehen: Großbritannien, Rumänien, Bulgarien

1.2.7. Keine Speicherung von Daten außerhalb des Firmennetzwerkes des Auftragnehmers

2. Dokumentationen des Auftragnehmers

Die vorgenannten und im Folgenden aufgeführten Dokumentationen sind vor Vertragsabschluss dem Auftraggeber vorzulegen und werden zum Vertragsgegenstand.

2.1. Verbindliche Vereinbarung zwischen dem Auftragnehmer und seinen Mitarbeitern mit Verweis auf die im „Konzept zum Betrieb von mobilen Arbeitsplätzen“ (s. u.) vorgegebenen Maßnahmen

2.2. Konzept zum Betrieb von mobilen Arbeitsplätzen mit folgenden Mindestinhalten:

- Maßgaben zum Datenschutz und zur Datensicherheit (z. B. im häuslichen Umfeld, auf Reisen, bei Verlust von Hardware und/oder Daten, zur Verschlüsselung von Daten, zur Datensicherung, ...) s. hierzu auch die Punkte 1.2.1 – 1.2.8
- Info an Auftraggeber, wenn Daten abhanden kommen oder Verstöße gegen die technisch-/organisatorischen Maßnahmen gem. Art. 32 DSGVO bei Vor-Ort-Kontrollen festgestellt werden
- Klärung der Vorgehensweise bei Schäden an vom Arbeitgeber überlassener Hardware
- Zutrittsrecht (Zutritt des Arbeitgebers, Auftraggebers und von Aufsichtsbehörden soweit sachlich notwendig) für Kontrollen der Gegebenheiten vor Ort
- Zusicherung des Beschäftigten des Auftragnehmers, dass die anderen Bewohner der Wohnung mit dieser Regelung einverstanden sind
- Durchgriffsrecht auf im BYOD-Modus eingebrachte Privatgeräte (z. B. zur Kontrolle der Einhaltung der Maßgaben, zur Löschung von Daten des Auftraggebers bei Verlust/Beendigung des Vertragsverhältnisses, ...)
- Vorgaben zur Anwendung von Vorkehrungen gegen die Einsichtnahme in Daten in DV-Geräten bei Nutzung im öffentlichen Bereich (z. B. Sichtschutzfolien für Laptops in öffentlichen Verkehrsmitteln oder anderen Orten mit Publikumsverkehr)

2.3. Dokumentation des Auftragnehmers über die durchgeführten Sicherheits- und Vor-Ort-Kontrollen (auf Verlangen dem Auftraggeber vorzulegen)

Geheimnisschutz nach § 203 Strafgesetzbuch (StGB)

Anhang C

1. Für die ordnungsgemäße Auftragsdurchführung ist es erforderlich, dass dem Auftragnehmer Daten bzw. Informationen übermittelt oder zugänglich gemacht werden, die dem besonderen Geheimnisschutz des § 203 deutsches Strafgesetzbuch (StGB) unterliegen (im Folgenden: „**Geheimnisse**“). Dieser strafrechtliche Geheimnisschutz lässt die datenschutzrechtlichen und sonstigen Bestimmungen und Verpflichtungen zur Vertraulichkeit unberührt. Die vorliegende Regelung konkretisiert die Pflichten des Auftragnehmers, seiner Organmitglieder, Mitarbeiter und der sonstigen vom Auftragnehmer im Rahmen dieses Vertrages eingesetzten Personen (z.B. Erfüllungsgehilfen/Subunternehmer, Verrichtungsgehilfen, sonstige Dienstleister und deren Mitarbeiter), denen in diesem Zusammenhang Geheimnisse offenbart werden - im Folgenden zusammen die „**mitwirkenden Personen“** - zum Geheimnisschutz nach § 203 StGB.

2. **Geheimnisse** sind alle nicht öffentlichen Informationen über Versicherungsnehmer und/oder Versicherte, die diesen Personen und/oder Unternehmen konkret zugeordnet werden können. Der Geheimnisschutz beschränkt sich daher nicht auf Gesundheitsdaten o.ä., sondern umfasst u.a. auch die Tatsache des Bestehens des Versicherungsvertrages.

3. Der Auftragnehmer wird hiermit darauf hingewiesen, dass die mitwirkenden Personen strenges Stillschweigen über die Geheimnisse wahren müssen und diese Dritten nicht offenbaren bzw. zugänglich machen dürfen. Dies gilt auch über das Ende der Mitwirkung hinaus. Als Dritte gelten auch solche Mitarbeiter des Auftragnehmers oder der Subdienstleister, die keine Kenntnis von den Geheimnissen im Rahmen der Auftragserfüllung benötigen. Diese Geheimnisschutzverpflichtung der mitwirkenden Personen ist strafrechtlich sanktioniert (§ 203 Abs. 4 Satz 1 StGB).

4. Der Auftragnehmer ist verpflichtet, dafür zu sorgen, dass sich die mitwirkenden Personen vor der erstmaligen Aufnahme ihrer Tätigkeit schriftlich auf die Geheimhaltung gemäß Ziff. 3 verpflichten, dabei insbesondere auch auf die Strafbarkeit einer unbefugten Geheimnisoffenbarung hingewiesen werden, und dass etwaige Subauftragnehmer von ihren mitwirkenden Mitarbeitern oder etwaigen weiteren Subauftragnehmern entsprechende Verpflichtungserklärungen einholen. Diese Verpflichtungserklärungen sind auf Verlangen des Auftraggebers nachzuweisen.

5. Der Auftragnehmer hat dafür Sorge zu tragen, dass die mitwirkenden Personen nur Zugriff auf die Daten haben, die sie zur Erbringung ihrer jeweils konkreten Aufgabe benötigen. Der Auftragnehmer und die mitwirkenden Personen dürfen sich nur insoweit Kenntnis von Daten/ Informationen verschaffen bzw. auf diese zugreifen, als dies zur jeweiligen Vertragsdurchführung erforderlich ist.

6. Der Auftragnehmer wird durch angemessene technische und organisatorische Maßnahmen den Schutz der Geheimnisse gegen unbefugte Kenntnisnahme sowie unbefugten Umgang sicherstellen bzw. - im Falle von Unterbeauftragungen - sicherstellen lassen.

7. Der Auftraggeber ist berechtigt, entweder selbst oder durch einen beauftragten Dritten auch vor Ort beim Auftragnehmer oder etwaigen Subauftragnehmern zu überprüfen, ob die Auftragserfüllung unter Einhaltung der vorliegenden Verpflichtungen erfolgt. Der Auftragnehmer muss in seinen vertraglichen Vereinbarungen mit Subauftragnehmern, soweit diesen befugterweise Geheimnisse offenbart werden, dem Auftraggeber das gleiche Prüfungsrecht direkt gegenüber den Subauftragnehmern einräumen.

8. Die vorstehenden Regelungen zum Geheimnisschutz begründen kein Recht auf Einschaltung von Subunternehmern; dies richtet sich nach dem Vertrag im Übrigen bzw. nach den Einzelverträgen.

9. Sonstige Vertraulichkeits- und Datensicherheitsvorgaben aus diesem Vertrag, aus den Einzelverträgen oder den Datenschutzvereinbarungen bleiben unberührt.

Technische und organisatorische Maßnahmen zu Datenschutz und Datensicherheit

Anhang E

Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung nachfolgender technischer und organisatorischer Maßnahmen nach dem Stand der Technik:

1 Vertraulichkeit

1.1 Zutrittskontrolle

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

Es werden ausschließlich von STRATO AG Pascalstraße 10 10587 Berlin und 1&1 Ionos SE Elgendorfer Str. 57 56410 Montabaur betriebene Datenverarbeitungsanlagen verwendet.

1.2 Zugangskontrolle

Maßnahmen, mit denen die Nutzung von Datenverarbeitungssystemen durch Unbefugte verhindert werden:

Authentifizierung gegenüber den verwendeten Datenverarbeitungssystemen erfolgt über von STRATO AG und 1und1 IONOS SE angebotene Infrastruktur (SSH mit RSA, sowie Basisauthentifizierung mit Benutzername/Passwort)

1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der Verarbeitung nicht unbefugt, gelesen, kopiert, verändert oder entfernt werden können:

Die Authorisierung zum lesenden oder schreibenden Zugriff auf Daten erfolgt ausschließlich für vom authentifizierten Benutzer selbst erstellten personenbezogenen Daten.

1.4 Trennungsgebot

Maßnahmen, die sicherstellen, dass Daten die zu unterschiedlichen Zwecken übermittelt wurden, auch getrennt verarbeitet werden:

Die Trennung eingegebener Datensätze wird durch die Anwendung ermöglicht (“Kampagnen”), jedoch nicht erzwungen.

1.5 Pseudonymisierung

Maßnahmen, die sicherstellen, dass personenbezogene Daten in einer Weise verarbeitet werden, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen

betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen:

Es besteht die Möglichkeit, Aufrufstatistiken über personalisierte Links, ausschließlich anonymisiert an den Benutzer zurückzumelden (Aggregation über die Anzahl).

1 Integrität

1.6 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:

Sämtliche Datenverbindungen zwischen dem Datenverarbeitenden System und Endbenutzern erfolgen über TLS-gesicherte Verbindungen.

1.7 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt werden können:

Sämtliche von Benutzern eingegebenen personenbezogenen Daten können ausschließlich vom eingebenden Benutzer selbst eingegeben, verändert oder entfernt werden.

2 Verfügbarkeit und Belastbarkeit

1.8 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

Manuelle Sicherung der Anwendungsdaten, sowie Konfigurationsdateien in ein externes Versionierungssystem (git).

1.9 Rasche Wiederherstellbarkeit

Vorkehrungen, die gewährleisten, dass die Daten möglichst schnell wieder zur Verfügung stehen:

Automatisierung und Dokumentation zur Inbetriebnahme des Gesamtsystems.
Versionierung sämtlicher Quellen, sowie Konfigurationsdateien.

3 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

1.10 Datenschutz Management

Darstellung der technischen und organisatorischen Vorkehrungen, die getroffen wurden um die Sicherheit der Daten nach dem Stand der Technik zu gewährleisten:

Ablage der Daten erfolgt auf einem zugangsbeschränkten Webserver (betrieben von STRATO AG 1und1 Ionos SE). Zugang ist ausschließlich durch Authentifizierung (RSA + Benutzername/Passwort) möglich. Die nötigen Geheimnisse zum Zugang sind

ausschließlich von Terminmaschine beauftragen Administratoren bekannt. Sämtliche Interaktionen mit dem Webserver erfolgen ausschließlich über verschlüsselnde Protokolle (SSH, SFTP). Zugriff auf über die Anwendung verwaltete Benutzerdaten erfolgt ausschließlich nach Authentifizierung über eine TLS-gesicherte Verbindung. Sämtliche Datenübertragungen zwischen Verwendern und dem Datenverarbeitungssystem erfolgen über TLS-gesicherte Verbindungen.

1.11 Datenschutzfreundliche Voreinstellungen

Wie wird gewährleistet, dass per Default-Einstellungen die Datenschutzschutzbelange gewahrt werden:

Standardmäßig werden für personenbezogenene Links anonymisierte Aufrufstatistiken verwendet.

1.12 Auftragskontrolle

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

Verwender erhalten vollständigen Zugriff auf von Ihnen eingegebene personenbezogene Daten. Jegliche Datenverarbeitung findet ausschließlich mittelbar oder unmittelbar durch den Verwender durchgeführte Eingaben statt.

Anhang F

Folgende Unternehmen sind zur Durchführung des vereinbarten Auftrages zur Datenverarbeitung als Subunternehmen von unserem Auftragnehmer eingesetzt:

Name und Sitz der Firma **(Vollständige Kontaktdaten)**	**Art und Zweck der Datenverarbeitung und die dazu übermittelten Daten**	**Betrieblicher Datenschutzbeauftragter** **(Vollständige Kontaktdaten)**
STRATO AG Pascalstraße 10 10587 Berlin	Serverhosting Inhaltsdaten, Nutzungsdaten, Verkehrsdaten	STRATO AG Pascalstraße 10 10587 Berlin
1&1 Ionos SE Elgendorfer Str. 57 56410 Montabaur	Serverhosting Inhaltsdaten, Nutzungsdaten, Verkehrsdaten	1&1 Ionos SE Elgendorfer Str.57 56410 Montabaur
Digistore24 GmbH St.-Godehard-Straße 32 31139 Hildesheim	Rechnungsdaten Vertragsdaten	Digistore24 GmbH St.-Godehard-Straße 32 31139 Hildesheim
Google Ireland Limited Gordon House, Barrow Street Dublin 4	Verkehrsdaten Webserver	Google Ireland Limited Gordon House, Barrow Street Dublin 4
sms77 e.K. Christian Leo Willestr. 4-624103 Kiel	Telekommunikationsdaten	sms77 e.K. Christian Leo Willestr. 4-624103 Kiel
Vimeo, Inc. 555 West 18th Street New York, New York 10011	Verkehrsdaten Video	Vimeo, Inc. Attention: Data Protection Officer 555 West 18th Street New York, New York 10011 Privacy@vimeo.com