



Anhang II
Vertrag über die Verarbeitung von
Daten im Auftrag (AVV)

Inhaltsverzeichnis

3	§ 1 Allgemeines
	§ 2 Rechte und Pflichten des Auftraggebers
	§ 3 Allgemeine Pflichten des Auftragnehmers
4	§ 4 Datenschutzbeauftragter des Unternehmens
	§ 5 Meldepflichten des Auftragnehmers
5	§ 6 Mitwirkungspflichten des Auftragnehmers
	§ 7 "Home-Office"-Regelungen
6	§ 8 Kontrollbefugnisse
	§ 9 Unterauftragsverhältnisse
7	§ 10 Vertraulichkeitsverpflichtung
	§ 11 Wahrung von Betroffenenrecht
	§ 12 Geheimhaltungspflichten
	§ 13 Vergütung
	§ 14 Technische und organisatorische Maßnahmen zur Datensicherheit (TOM)
8	§ 15 Dauer des Auftrags
	§ 16 Beendigung
	§ 17 Schlussbestimmungen
9	Anlage 1 – Gegenstand des Auftrags u.a.
10	Anlage 2 – Unterauftragnehmer
11	Anlage 3 – Allgemeine technische und organisatorische Maßnahmen (TOM) nach Art. 25 und Art. 32 DSGVO

Geschlechtsneutrale Sprachform

Aus Gründen der leichteren Lesbarkeit wird die männliche Sprachform bei personenbezogenen Substantiven und Pronomen verwendet. Dies impliziert jedoch keine Benachteiligung des weiblichen Geschlechtes, sondern soll im Sinne der sprachlichen Vereinfachung als geschlechtsneutral zu verstehen sein.

Vertrag über die Verarbeitung von Daten im Auftrag (AVV)

Zwischen Auftraggeber

Name StBG/-sozietät: _____
Straße, Hausnummer: _____
PLZ, Ort: _____
vertreten durch: _____

– nachstehend Auftraggeber/Kunde genannt –

und Auftragnehmer

buchhalter.pro GmbH
Hopfenstraße 1a–d
24114 Kiel
vertreten durch: Geschäftsführer Carsten Koch

– nachstehend Auftragnehmer/buchhalter.pro genannt –

wird dieser Vertrag über folgende Dienstleistung abgeschlossen:

§ 1 Allgemeines

- (1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.
- (2) 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.

Gegenstand des Auftrags

Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in **Anlage 1** zu diesem Vertrag in der Leistungsbeschreibung festgelegt.

§ 2 Rechte und Pflichten des Auftraggebers

- (1) Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht nach Ziff. 4 Abs. 5 das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.
- (2) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte im Zusammenhang mit dieser Verarbeitung von Daten im Auftrag gegenüber dem Auftragnehmer geltend machen.
- (3) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen müssen in Textform (z.B. E-Mail) erfolgen.
- (4) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.
- (5) Der Auftraggeber kann weisungsberechtigte Personen benennen. Sofern weisungsberechtigte Personen benannt werden sollen, werden diese in der **Anlage 1** benannt. Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer in Textform mitteilen.
- (6) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.
- (7) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich

§ 3 Allgemeine Pflichten des Auftragnehmers

- (1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der

Datenverarbeitung richten sich ansonsten 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.

- (2) Der Auftragnehmer verpflichtet sich, die Datenverarbeitung im Auftrag nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen. Eine Verarbeitung der personenbezogenen Daten in einem Drittland bedarf der vorherigen Zustimmung des Auftraggebers, die zumindest in Textform (z.B. E-Mail) erfolgen muss.

Eine Zustimmung des Auftraggebers kommt nur dann in Betracht, wenn gewährleistet ist, dass die jeweils nach den Art. 44 – 49 DSGVO einzuhaltenden Rechtsvorschriften eingehalten werden, um ein angemessenes Schutzniveau für den Schutz der personenbezogenen Daten zu gewährleisten.
- (3) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu.
- (4) Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. Der Auftragnehmer wird Änderungen in der Organisation der Datenverarbeitung im Auftrag, die für die Sicherheit der Daten erheblich sind, vorab mit dem Auftraggeber abstimmen.
- (5) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.
- (6) Die Verarbeitung von Daten im Auftrag des Auftraggebers außerhalb von Betriebsstätten des Auftragnehmers oder Subunternehmern ist nur mit Zustimmung des Auftraggebers in Schriftform oder Textform zulässig. Eine Verarbeitung von Daten für den Auftraggeber in Privatwohnungen ist nur mit Zustimmung des Auftraggebers in Schriftform oder Textform im Einzelfall zulässig.
- (7) Der Auftragnehmer wird die Daten, die er im Auftrag für den Auftraggeber verarbeitet, getrennt von anderen Daten verarbeiten. Eine physische Trennung ist nicht zwingend erforderlich.
- (8) Der Auftragnehmer kann dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind. Sofern weisungsempfangsberechtigte Personen benannt werden sollen, werden diese in der **Anlage 1** benannt. Für den Fall, dass sich die weisungsempfangsberechtigten Personen beim Auftragnehmer ändern, wird der Auftragnehmer dies dem Auftraggeber in Textform mitteilen.

§ 4 Datenschutzbeauftragter des Auftragnehmers

- (1) Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat. Der Auftragnehmer trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt.

Kontaktdaten der Datenschutzbeauftragten des Auftragnehmers:

Datenschutz Vogel
RA Andre Vogel
Markt 15
23701 Eutin
04521-3661
04521-3667 (Fax)
av@datenschutz-eutin.de

- (2) Die Pflicht zur Benennung eines Datenschutzbeauftragten nach Absatz 1 kann im Ermessen des Auftraggebers entfallen, wenn der Auftragnehmer nachweisen kann, dass er gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu benennen und der Auftragnehmer nachweisen kann, dass betriebliche Regelungen bestehen, die eine Verarbeitung personenbezogener Daten unter Einhaltung der gesetzlichen Vorschriften, der Regelungen dieses Vertrages sowie etwaiger weiterer Weisungen des Auftraggebers gewährleisten.

§ 5 Meldepflichten des Auftragnehmers

- (1) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet.

(1a) Der Auftragnehmer kommt seiner Meldeverpflichtung gegenüber dem Auftraggeber dadurch nach, dass dieser per E-Mail informiert wird. Zusätzlich wird der benannte Weisungsberechtigte durch einen mitteilenden Anruf, ein Faxschreiben oder in Schriftform, wobei diese mittels Einschreiben zu erfolgen hat informiert werden.

Die Vornahme der Information und der Kenntnisnahme durch den benannten Weisungsberechtigten oder eines von ihm benannten Dritten wird durch den Auftragnehmer dokumentiert werden.

(2) Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann.

(3) Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht im Falle von Datenschutzverletzungen nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich, spätestens aber binnen 48 Stunden ab Kenntnis des Zugriffs mitteilen. Die Meldung des Auftragnehmers an den Auftraggeber muss insbesondere folgende Informationen beinhalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

§ 6 Mitwirkungspflichten des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO. Es gelten die Regelungen von Ziff. 12 dieses Vertrages.

(2) Der Auftragnehmer wirkt an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten durch den Auftraggeber mit. Er hat dem Auftraggeber die insoweit jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

(3) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

§ 7 „Home-Office“-Regelung

(1) Der Auftragnehmer darf seinen Beschäftigten, die mit der Verarbeitung von personenbezogenen Daten für den Auftraggeber beauftragt sind, mit vorheriger Zustimmung des Auftraggebers die Verarbeitung von personenbezogenen Daten in Privatwohnungen („Home-Office“) erlauben. Die Zustimmung des Auftraggebers bedarf der Textform (z.B. E-Mail).

Der Auftraggeber genehmigt die Verarbeitung von personenbezogenen Daten durch die Beschäftigten des Auftragnehmers im Homeoffice bereits jetzt für den Fall höherer Gewalt oder bei behördlichen Maßnahmen, wie beispielsweise Kontaktsperren, Ausgangssperren, amtliche Reisewarnungen, Einstufung der WHO als gesundheitliche Notlage mit internationaler Tragweite.

(2) Der Auftragnehmer hat sicherzustellen, dass die Einhaltung der vertraglich vereinbarten technischen und organisatorischen Maßnahmen auch im „Home-Office“ der Beschäftigten des Auftragnehmers gewährleistet ist. Abweichungen von einzelnen vertraglich vereinbarten technischen und organisatorischen Maßnahmen sind vorab mit dem Auftraggeber abzustimmen und von diesem in Textform zu genehmigen.

(3) Der Auftragnehmer trägt insbesondere Sorge dafür, dass bei einer Verarbeitung von personenbezogenen Daten im „Home-Office“ die Speicherorte so konfiguriert werden, dass eine lokale Speicherung von Daten auf IT-Systemen, die im „Home-Office“ verwendet werden, ausgeschlossen ist. Sollte dies nicht möglich sein, hat der Auftragnehmer Sorge dafür zu tragen, dass die lokale Speicherung ausschließlich verschlüsselt erfolgt und andere im Haushalt befindliche Personen keinen Zugriff auf diese Daten erhalten.

(4) Der Auftragnehmer ist verpflichtet, Sorge dafür zu tragen, dass eine wirksame Kontrolle der Verarbeitung personenbezogener Daten im Auftrag im „Home-Office“ durch den Auftraggeber möglich ist. Dabei sind die Persönlichkeitsrechte der Beschäftigten sowie der weiteren im jeweiligen Haushalt lebenden Personen angemessen zu berücksichtigen.

(5) Sofern auch bei Unterauftragnehmern Beschäftigte im „Home-Office“ eingesetzt werden sollen, gelten die Regelungen der Absätze 1 bis 4 entsprechend.

§ 8 Kontrollbefugnisse

- (1) Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren.
- (2) Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.
- (3) Der Auftraggeber kann eine Einsichtnahme in die vom Auftragnehmer für den Auftraggeber verarbeiteten Daten sowie in die verwendeten Datenverarbeitungssysteme und -programme verlangen.
- (4) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören.
- (5) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende geplante Maßnahmen vom Auftragnehmer zu informieren.
- (6) Die Parteien sind sich darüber einig, dass die Kontrollmaßnahmen bei einer Verarbeitung von personenbezogenen Daten im „Home-Office“ zur Wahrung der Persönlichkeitsrechte von Beschäftigten des Auftragnehmers und etwaiger weiterer Personen im jeweiligen Haushalt primär durch eine Kontrolle der Sicherstellung der vom Auftragnehmer nach Ziff. 8 Abs. 2 und 3 zu treffenden Maßnahmen erfolgt. Anlassbezogen ist dem Auftraggeber auch eine Kontrolle im „Home-Office“ von Beschäftigten durch den Auftragnehmer zu ermöglichen.

§ 9 Unterauftragsverhältnisse

- (1) Die Beauftragung von Unterauftragnehmern durch den Auftragnehmer ist nur mit Zustimmung des Auftraggebers in Textform zulässig. Der Auftragnehmer wird alle bereits zum Vertragsschluss bestehenden Unterauftragsverhältnisse in der **Anlage 2** zu diesem Vertrag angeben.
- (2) Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln.
- (3) Der Auftragnehmer ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen Datenschutzbeauftragten gemäß Art. 37 DSGVO benannt hat. Für den Fall, dass kein Datenschutzbeauftragter beim Unterauftragnehmer benannt worden ist, hat der Auftragnehmer den Auftraggeber hierauf hinzuweisen und Informationen dazu beizubringen, aus denen sich ergibt, dass der Unterauftragnehmer gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu benennen.
- (4) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten.
- (5) Der Auftragnehmer hat mit dem Unterauftragnehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat der Auftragnehmer dem Unterauftragnehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Auftraggeber und Auftragnehmer festgelegt sind. Dem Auftraggeber ist der Auftragsdatenverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.
- (6) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 9 dieses Vertrages) des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.
- (7) Nicht als Unterauftragsverhältnisse i.S.d. Absätze 1 bis 6 sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten. Die Wartung und Pflege von IT-System oder Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis und Auftragsverarbeitung i.S.d. Art. 28 DSGVO dar, wenn die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden und bei der Wartung auf personenbezogenen Daten zugegriffen werden kann, die im Auftrag des Auftraggebers verarbeitet werden.
- (8) Bei einem datenschutzrechtlichen Fehlverhalten des Unterauftragnehmers, haftet der Auftragnehmer für dieses Fehlverhalten nach den gesetzlichen Regelungen.

§ 10 Vertraulichkeitsverpflichtung

- (1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber ist verpflichtet, dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitzuteilen.
- (2) Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass er seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und zur Vertraulichkeit verpflichtet hat. Der Auftragnehmer sichert ferner zu, dass er insbesondere die bei der Durchführung der Arbeiten tätigen Beschäftigten zur Vertraulichkeit verpflichtet hat und diese über die Weisungen des Auftraggebers informiert hat.
- (3) Die Verpflichtung der Beschäftigten nach Absatz 2 sind dem Auftraggeber auf Anfrage nachzuweisen.

§ 11 Wahrung von Betroffenenrechten

- (1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützen. Der Auftragnehmer hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.
- (2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten – insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung – durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.
- (3) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer entstehen, bleiben unberührt.
- (4) Für den Fall, dass ein Betroffener seine Rechte nach den Art. 12-23 DSGVO beim Auftragnehmer geltend macht, obwohl dies offensichtlich eine Verarbeitung personenbezogener Daten betrifft, für die der Auftraggeber verantwortlich ist, ist der Auftragnehmer berechtigt, dem Betroffenen mitzuteilen, dass der Auftraggeber der Verantwortliche für die Datenverarbeitung ist. Der Auftragnehmer darf dem Betroffenen in diesem Zusammenhang die Kontaktdaten des Verantwortlichen mitteilen.

§ 12 Geheimhaltungspflichten

- (1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.
- (2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

§ 13 Vergütung

Etwaige Regelungen zu einer Vergütung von Leistungen sind zwischen den Parteien gesondert zu vereinbaren.

§ 14 Technische und organisatorische Maßnahmen zur Datensicherheit (TOM)

- (1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.
- (2) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als **Anlage 3** zu diesem Auftragsverarbeitungsvertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Voraus mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.
- 3 Der Auftragnehmer wird die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig und auch anlassbezogen auf ihre Wirksamkeit kontrollieren. Für den Fall, dass es Optimierungs- und/oder Änderungsbedarf gibt, wird der Auftragnehmer den Auftraggeber informieren.

§ 15 Dauer des Auftrags

- (1) Der Vertrag beginnt mit Unterzeichnung und wird auf unbestimmte Zeit geschlossen.
- (2) Er ist mit einer Frist von einem Monat zum Monatsende kündbar.
- (3) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

§ 16 Beendigung

- (1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt. Für Datenträger gilt, dass diese im Falle einer vom Auftraggeber gewünschten Löschung zu vernichten sind, wobei mindestens die Sicherheitsstufe 3 der DIN 66399 einzuhalten ist; die Vernichtung ist dem Auftraggeber unter Hinweis auf die Sicherheitsstufe gemäß DIN 66399 nachzuweisen.
- (2) Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragnehmers erfolgen. Die Vor-Ort-Kontrolle soll mit angemessener Frist durch den Auftraggeber angekündigt werden.
- (3) Der Auftragnehmer darf personenbezogene Daten, die im Zusammenhang mit dem Auftrag verarbeitet worden sind, über die Beendigung des Vertrages hinaus speichern, wenn und soweit den Auftragnehmer eine gesetzliche Pflicht zur Aufbewahrung trifft. In diesen Fällen dürfen die Daten nur für Zwecke der Umsetzung der jeweiligen gesetzlichen Aufbewahrungspflichten verarbeitet werden. Nach Ablauf der Aufbewahrungspflicht sind die Daten unverzüglich zu löschen.

§ 17 Schlussbestimmungen

- (1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.
- (2) Die Einrede des Zurückbehaltungsrechts i.S.v. § 27 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der dazugehörigen Datenträger ausgeschlossen.
- (3) Für Nebenabreden ist die Schriftform erforderlich.
- (4) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

_____, den _____
Ort Datum

Name und Funktion Auftraggeber/Kunde

Unterschrift Auftraggeber/Kunde

Kiel _____, den _____
Ort Datum

Carsten Koch, Geschäftsführer

Name und Funktion Auftragnehmer/buchhalter.pro

Unterschrift Auftragnehmer/buchhalter.pro

Vertrag über die Verarbeitung von Daten im Auftrag (AVV)

Anlage 1 – Gegenstand des Auftrags u.a.

1. Gegenstand und Zweck der Verarbeitung

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Arbeiten und/oder Leistungen, welche sich aus der dem zwischen den Parteien geschlossenen Dienstleistungsvertrag und dort aus der beigefügten Leistungsbeschreibung ergeben.

Art(en) der personenbezogenen Daten

Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

- a) Namen
- b) Adressen
- c) Kontaktdaten (Telefon- und Faxnummer, E-Mail-Adressen)
- d) Geburtsdaten
- e) Lohn- und Gehaltsdaten (Bruttobezüge, Abgaben, Nettobezüge)
- f) Arbeitszeiten
- g) Daten für die Lohnsteuerberechnung (Steuer-ID, Steuerklasse, Religion u.a.)
- h) Sozialversicherungsdaten (SV-Nr., Krankenkasse, SV-Schlüssel u.a.)
- i) Ausbildungen, Qualifikationen, ausgeübte Tätigkeiten
- j) Daten über das Beschäftigungsverhältnis (Beginn, Ende, u.a.)
- k) Vertragsdaten (Arbeitsverträge, Gesellschafterverträge, Geschäftsführerverträge, Altersvorsorgeverträge, u.a.)
- l) Name und Alter von Angehörigen soweit für Sozialleistungen relevant
- m) Gesundheitsdaten soweit für die Lohnabrechnung Abgaben relevant
- n) Bankverbindungen inklusive Kontodaten bzw. -umsätze
- o) Schwerbehinderungen

Kategorien betroffener Personen

Kreis der von der Datenverarbeitung betroffenen Personen:

- a) Kunden/Mandanten/Klienten/Kanzleien (Steuerberater)
- b) Mitarbeiter, Auszubildende, Praktikanten, Ruheständler, Unterhaltsberechtigte, Geschäftsführer, geschäftsführende Gesellschafter, freie Mitarbeiter, Handelsvertreter (jeweils früher, aktuell, zukünftig in a) tätig)

Weisungsberechtigte Personen des Auftraggebers

Name und Funktion Person 1

Name und Funktion Person 2

Name und Funktion Person 3

Name und Funktion Person 4

Weisungsempfangsberechtigte Personen des Auftragnehmers

Als weisungsberechtigte Person tritt für die buchhalter.pro GmbH der/die jeweilige GeschäftsführerIn auf.

Vertrag über die Verarbeitung von Daten im Auftrag (AVV) Anlage 2 – Unterauftragnehmer

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“).

Dabei handelt es sich um nachfolgende(s) Unternehmen:

KEINE

Vertrag über die Verarbeitung von Daten im Auftrag (AVV)

Anlage 3 – Allgemeine technische und organisatorische Maßnahmen (TOM) nach Art. 25 und Art. 32 DSGVO

1. Zutrittskontrolle

Der Auftragnehmer hat folgende Maßnahmen getroffen, um einen Zutritt unbefugter Personen zu verhindern:

- Bei Abwesenheit aller Mitarbeiter werden die Geschäftsräume verschlossen.
- Nur Berechtigte Personen haben Schlüssel für die Geschäftsräume
- Der Hauseingang ist außerhalb der Geschäftszeiten geschlossen. Das Gebäude kann dann nur mit Schlüssel oder von Innen mittels Türöffner geöffnet werden.
- Der Serverraum ist verschlossen. Zutritt zum Serverraum haben nur Mitarbeiter, die mit Aufgaben betraut sind, die einen Zutritt erfordern.

2. Zugangskontrolle

Der Auftragnehmer hat folgende Maßnahmen getroffen, um ein Eindringen Unbefugter in die DV-Systeme zu verhindern:

- Die Anmeldung an allen Arbeitsstationen bzw. an den datentragenden Programmen ist nur mit den korrekten Anmeldedaten (Benutzername und Passwort – double verifikation) möglich.
- Die verwendeten Passwörter haben mindestens 8 Zeichen.
- Die Passwörter werden mindestens einmal jährlich geändert.
- Alle Daten befinden sich in einer gesicherten Serverumgebung.
- Daten, die sich außerhalb der Serverumgebung befinden (Datensicherungen) werden verschlüsselt.

3. Zugriffskontrolle

Der Auftragnehmer hat folgende Maßnahmen getroffen, um unerlaubte Tätigkeiten außerhalb der eingeräumten Berechtigungen zu verhindern:

- Jeder Benutzer erhält nur die Zugriffsrechte auf Verzeichnisse und Datenbanken, die er für seine Tätigkeit benötigt bzw. für die eine entsprechende Zugriffsberechtigung eingerichtet wurde.

4. Weitergabekontrolle

Der Auftragnehmer hat folgende Maßnahmen zur Regelung der Weitergabe personenbezogener Daten getroffen:

- Soweit personenbezogene Daten an externe Anspruchsstellen übermittelt werden, erfolgt deren Übertragung über eine sichere Verbindung und/oder mittels der durch den Gesetzgeber vorgesehenen Verschlüsselungsverfahren. (Sozialversicherung: ITSG-Zertifikat, Finanzbehörden: ELSTER-Zertifikat)
- Bevor personenbezogene Daten an den Auftraggeber übermittelt werden, werden die Daten mittels PGP verschlüsselt oder die Übertragung findet über eine sichere Verbindung statt.
- Eine elektronische Übermittlung von Daten an andere Empfänger (z.B. Mitarbeiter des Auftraggebers) findet nicht statt.

5. Eingabekontrolle

Der Auftragnehmer hat folgende Maßnahmen ergriffen, um die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege sicherzustellen:

- Alle in den Datenbanken vorgenommenen Datenmanipulationen (Anlegen, Löschen, Ändern von Datensätzen) werden revisionssicher protokolliert.

6. Verfügbarkeitskontrolle

Der Auftragnehmer hat folgende Maßnahmen ergriffen, um Daten gegen zufällige Zerstörung oder Verlust zu schützen:

- tägliches vollständiges Backup innerhalb des Serversystems
- tägliches vollständiges, verschlüsseltes, Backup auf externen Datenträger
- Aufbewahrung der aktuellen externen Datenträger außer Haus
- Regelmäßige persönliche Kontrolle der Datensicherung durch geschultes Personal
- Einsatz professionelle Antiviren- und Firewall Software auf dem Serversystem und auf allen Arbeitsplätzen.

7. Trennungskontrolle

Tests erfolgen in, vom Produktivsystem getrennten, EDV-Systemen.