# Vereinbarung zur Auftragsverarbeitung (VAV)

personenbezogener Daten im Auftrag gemäß Art. 28 der europäischen Datenschutzgrundverordnung (EU-DSGVO) vom 28.05.2020

**Präambel**

WIZARD COMPUTERSYSTEME GMBH („WIZARD“) ist auf die Betreuung von IT-Systemen bei Freiberuflern, mittelständischen Unternehmen, Steuerberatern und Wirtschaftsprüfern spezialisiert. Neben klassischen vor Ort IT-Servicearbeiten und Netzwerkbetreuungen beim Auftraggeber hat sich WIZARD auf das „Application-Service-Providing“ (ASP) spezialisiert und erbringt „Cloud-Computing“-Leistungen in zwei eigenen Rechenzentren in Bremervörde. Diese Vereinbarung konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Vertragspartner in Zusammenhang mit dem Umgang der Auftragnehmerseite mit personenbezogenen Daten.

**I. Begriffe**

Für diese *VAV* gelten die nachstehend definierten Begriffe; diese werden in *Kursivdruck* hervorgehoben.

1. ***„Personenbezogene Daten"*** (Art. 4 Nr. 1 EU-DSGVO) sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (nachfolgend *„betroffene Person"* genannt) beziehen. 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 identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

2. ***„Hauptvertrag“*** bezeichnet eine Vereinbarung zwischen den Vertragspartnern über die Erbringung von Leistungen der in der Präambel bezeichneten Art. Es können mehrere Hauptverträge parallel bestehen. Der *Hauptvertrag* kann bestehen aus einem Angebot, einer Auftragsbestätigung, einer schriftlichen oder mündlichen Beauftragung, einer sonstigen vertraglichen Vereinbarung, einer Leistungsbeschreibung und den Allgemeinen Geschäftsbedingungen von WIZARD sowie etwaigen Nachträgen und Zusatzvereinbarungen, alle Dokumente jeweils in der anwendbaren Fassung. Die Vereinbarung zur *Auftragsverarbeitung* gemäß Art. 28 EU-DSGVO gilt auch, sofern die Leistungsbeschreibungen und die jeweiligen Hauptverträge nicht ausdrücklich Bezug nehmen auf diese *VAV*.

3. ***„Auftraggeber-Daten“*** sind diejenigen gemäß einem *Hauptvertrag* im Auftrag zu *verarbeitenden personenbezogenen Daten*, für die der Auftraggeber Verantwortlicher ist.

4. ***„Besonders schützenswerte personenbezogene Daten“*** (Art. 9 EU-DSGVO) sind Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

5. ***„Verarbeitung"*** (bzw. in Verbform ***„verarbeiten“***) (Art. 4 Nr. 2 EU-DSGVO) ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit *Auftraggeber-Daten* wie Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form von Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschung oder Vernichtung. *Verarbeitung* meint dabei in erster Linie die vollständig oder teilweise automatisierte *Verarbeitung*, aber auch die nicht automatisierte *Verarbeitung* von Auftraggeber-Daten, die bereits in einer Datei gespeichert sind oder noch gespeichert werden sollen. *Verarbeitung* erfolgt vonseiten des Auftragnehmers unter einem *Hauptvertrag* nur als *Auftragsverarbeitung*.

6. ***„Verantwortlicher"*** (Art. 4 Nr. 7 EU-DSGVO) ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der *Verarbeitung* von *personenbezogenen Daten* entscheidet. *Verantwortlicher* unter dieser Vereinbarung bzw. unter einem *Hauptvertrag* ist der Auftraggeber.

7. ***„Dritter“*** (Art. 4 Nr. 10 EU-DSGVO) ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der *betroffenen Person*, dem Verantwortlichen, dem jeweiligen Auftragnehmer und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des jeweiligen Auftragnehmers befugt sind, die *Auftraggeber-Daten* zu *verarbeiten*.

8. ***„Auftragsverarbeitung“*** (bzw. in Verbform ***„im Auftrag verarbeiten“***) ist die *Verarbeitung* der *Auftraggeber-Daten* durch einen Auftragnehmer, und zwar ausschließlich nach Weisungen des Auftraggebers im Rahmen eines *Hauptvertrags* und dieser *VAV* sowie der wirksamen Einzelweisungen ergänzend im Rahmen der Vorgaben gemäß Art. 28, 29 EU-DSGVO.

9. ***„TOM“*** ist eine Abkürzung für ***„technische und/oder organisatorische Maßnahmen“*** (Art. 28 Abs. 3 S. 2 lit. c), Art. 32 EU-DSGVO) und meint auf Seiten von WIZARD, sofern nicht ausdrücklich anders beschrieben, die in dem Datenschutzkonzept von WIZARD niedergelegten Maßnahmen nach, Art. 32 EU-DSGVO, diese können jeweils aktuell unter **https://www.wizard.de** (unter *„TOM“*) eingesehen werden.

10. ***„DSB“*** ist die Abkürzung für ***„Datenschutzbeauftragter“***. Dies ist im Zweifel eine geeignete Institution bzw. Person gemäß Art. 37 bis 39 EU-DSGVO, § 38 BDSG.

11. ***„WIZARD-Produkt“*** ist eine Leistung oder ein Computerprogramm, das durch den Auftragnehmer selbst bzw. von einem Dritten in dessen Auftrag erstellt wurde und im Rahmen der Erbringung von Leistungen unter einem *Hauptvertrag* genutzt wird bzw. dessen Nutzung die Leistung darstellt.

12. Unter ***„VAV“*** wird diese „Vereinbarung zur *Auftragsverarbeitung* nach Art. 28 EU-DSGVO“ verstanden.

**II. Art, Umfang, Zweck, Laufzeit und Ort der Auftragsverarbeitung**

1. Der Auftragnehmer betreibt unter der *VAV* ausschließlich *Auftragsverarbeitung*. Der Auftraggeber bleibt Verantwortlicher (**„Herr der Daten“**).

2. Die Art der *Auftragsverarbeitung* umfasst diejenigen Arten von *Verarbeitungen*, die zur Erbringung der vereinbarten Leistungen gemäß dem jeweiligen *Hauptvertrag* erforderlich sind, sowie alle etwa in der jeweiligen Leistungsbeschreibung zu einem *Hauptvertrag* vereinbarten weiteren Vertragszwecke.

3. In heterogenen Umgebungen (z.B. Servicearbeiten im IT-System des Kunden) ist jeweils derjenige der verantwortliche *Auftragsdatenverarbeiter*, der die eigentliche Kontrolle über den jeweiligen Datenbereich in dem betreffenden Zeitraum ausübt. Der Auftraggeber hat (z.B. für eigene Serversysteme im eigenen Haus) eigene *TOM* zu veranlassen oder zu ergreifen.

4. Betroffene Daten sind alle Arten *personenbezogener Daten*, die ein Auftragnehmer im Auftrag des Auftraggebers *verarbeitet*. Hiervon umfasst sind gelegentlich auch besonders schützenswerte *personenbezogener Daten*. Für eine etwa notwendige Datenschutz-Folgenabschätzung (Art. 35 EU-DSGVO) ist allein der Auftraggeber verantwortlich; der Auftragnehmer leistet insoweit Unterstützung nach Maßgabe dieser *VAV*.

5. Hinsichtlich der *Verarbeitung* von *personenbezogenen Daten* über strafrechtliche Verurteilungen und Straftaten i.S.d. Art. 10 EU-DSGVO ist der Auftraggeber verpflichtet, in eigener Verantwortung dafür Sorge zu tragen, dass die hierzu geltenden gesetzlichen Vorgaben eingehalten werden.

6. Die Laufzeit der *Auftragsverarbeitung* ergibt sich aus dem jeweiligen *Hauptvertrag* und ist im Zweifel auf die Laufzeit des *Hauptvertrages* begrenzt.

7. **Die *Auftragsverarbeitung* findet ausschließlich in Deutschland statt!** Jede Verlagerung/Übermittlung in ein Drittland bedarf der vorherigen dokumentierten Zustimmung des Auftraggebers und darf nur erfolgen, wenn zuvor die besonderen Voraussetzungen der Art. 44 ff. EU-DSGVO erfüllt sind, d.h. ein angemessenes Schutzniveau nachgewiesen ist bzw. entsprechende Garantien bestehen.

**III. Weisungsbefugnisse des Auftraggebers**

1. Der Auftragnehmer *verarbeitet* die Auftraggeber-Daten ausschließlich in Übereinstimmung mit den Weisungen des Auftraggebers, wie sie – vorbehaltlich etwaiger wirksamer Einzelweisungen – abschließend in den Bestimmungen der *VAV* und im jeweiligen *Hauptvertrag* enthalten sind. Dies gilt insbesondere bei der Einrichtung von Benutzerverwaltungen (Login, Einwahlmöglichkeit, Nutzungskontrolle, Rechteverwaltung bzw. Zugriffsrechte auf Datenbestände, Programmfunktionen usw.).

Einzelweisungen, die von den im jeweiligen *Hauptvertrag* getroffenen Festlegungen abweichen oder im Verhältnis dazu zusätzliche bzw. veränderte Anforderungen aufstellen, bedürfen zu ihrer Wirksamkeit mindestens der Textform und, sofern und soweit

a) dadurch beim Auftragnehmer bestehende Arbeitsabläufe verändert werden,

b) sich der Aufwand beim Auftragnehmer erhöht oder

c) der Auftraggeber in der Weisung nicht darlegen kann, dass sich datenschutzrechtliche Risiken für den Auftragnehmer im Verhältnis zu dem jeweils vorangehenden Zustand nicht erhöhen, einer ausdrücklichen vorherigen Zustimmung seitens des Auftragnehmers, mindestens in Textform.

Solche Einzelweisungen erfolgen im Übrigen nach Maßgabe eines etwa im Hauptvertrag festgelegten Änderungsverfahrens. Mehraufwand, der durch die Übernahme der Abweichung oder Änderung aufgrund der Weisung des Auftraggebers bedingt sind, gehen zu dessen Lasten. Eine nicht mindestens in Textform erfolgende Einzelweisung ist unverzüglich in Textform durch den Auftraggeber zu bestätigen. Der Auftragnehmer ist berechtigt, die aufgrund einer Weisung geschuldete Tätigkeit auszusetzen, bis die dokumentierte Form der Weisung erfolgt ist.

Eine von wirksamen Weisungen bzw. Einzelweisungen abweichende *Auftragsverarbeitung* ist ausgeschlossen.

2. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen geltendes Datenschutzrecht verstößt, wird er gemäß Art. 28 Abs. 3 Satz 3 i.V.m. lit. h EU-DSGVO den Auftraggeber möglichst zeitnah, mindestens in Textform, darauf hinweisen. Außerdem ist der Auftragnehmer berechtigt, die Ausführung der Weisung bis zu einer dokumentierten Bestätigung der Weisung durch den Auftraggeber auszusetzen.

Folgt der Auftragnehmer nach der Bestätigung der Weisung durch den Auftraggeber der bestätigten Weisung, trägt der Auftraggeber alle damit etwa verbundenen Risiken, insbesondere betreffend der Einhaltung von Datenschutzvorschriften und der Ansprüche betroffener Personen. Dies gilt jedoch nicht, sofern und soweit eine von dem Auftragnehmer zu vertretende, inhaltlich fehlerhafte Ausführung der Weisung erfolgt. Der Auftragnehmer übernimmt keine Haftung für die Rechtmäßigkeit der erteilten Aufträge, es sei denn, dass für den Auftragnehmer spezifische Datenschutzvorschriften als Auftragsverarbeiter gelten und von diesem verletzt wurden.

3. Enthält ein *Hauptvertrag* keine Weisung und hat auch der Auftraggeber keine dokumentierte Einzelweisung erteilt, wie die *Verarbeitung*, insbesondere bei Datensicherungs-, Datenbankprüfungs-, Software-Installations- und Softwarepflege-Arbeiten, zu erfolgen hat, so wird diese, sofern der Auftraggeber nicht widerspricht und diesen Widerspruch dokumentiert, nach den jeweils anwendbaren dokumentierten Richtlinien und Empfehlungen der jeweiligen Softwarehersteller (z.B. Microsoft, DATEV usw.) und im Übrigen nach Verfahren gemäß dem aktuellen Stand der Technik bzw. der Sensibilität der personenbezogene Daten entsprechend angemessen vorgenommen. Bei einem Widerspruch wartet der Auftragnehmer eine dokumentierte Einzelweisung ab und wird bis dahin die von dem Widerspruch betroffene Leistung nicht erbringen.

4. Auf Seiten des Auftraggebers sind die weisungsbefugten Personen bzw. Rollen mitzuteilen.

**IV. Grundlegende Pflichten des Auftraggebers**

1. Der Auftraggeber ist im Rahmen der *VAV* für die Einhaltung der anwendbaren datenschutzrechtlichen Vorschriften allein verantwortlich, insbesondere für die Zulässigkeit und Rechtmäßigkeit der *Verarbeitung*. Dies gilt nicht, sofern und soweit der Auftragnehmer rechtmäßigen Weisungen des Auftraggebers zuwiderhandelt oder in zu vertretender Weise die für Auftragsverarbeiter anwendbaren Vorschriften des Datenschutzrechts bzw. diese *VAV* verletzt (Art. 82 Abs. 2 S. 2 EU-DSGVO).

2. Der Auftraggeber hat den Auftragnehmer sorgfältig ausgewählt. Er hat ihn sorgfältig zu überwachen und die Rechte der betroffenen Personen zu wahren. Er unterliegt der Aufsicht der Aufsichtsbehörden.

3. Sollten Dritte gegen den Auftragnehmer aufgrund der *Verarbeitung* von Auftraggeber-Daten Ansprüche geltend machen, wird der Auftraggeber den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen, sofern und soweit nicht Ziff. 1 Satz 2 eingreift.

4. Der Auftraggeber ist im Verhältnis der Vertragspartner zueinander Berechtigter bzgl. der Auftraggeber-Daten und Inhaber aller etwaiger Rechte, die die Auftraggeber-Daten betreffen.

5. Der Auftraggeber ist verpflichtet, dem Auftragnehmer die Auftraggeber-Daten rechtzeitig zur Leistungserbringung nach dem jeweiligen *Hauptvertrag* zur Verfügung zu stellen. Der Auftraggeber ist verantwortlich für die Qualität einschließlich der Aktualität und der Richtigkeit der zur Verfügung gestellten Auftraggeber-Daten.
6. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig in dokumentierter Form zu informieren, wenn er bei der Prüfung der Ergebnisse der Tätigkeiten des Auftragnehmers Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seiner Weisungen feststellt.
7. Der Auftraggeber ist gehalten, Protokolle von Leistungen, die sich auf personenbezogene Daten beziehen, unverzüglich zu überprüfen. Beanstandungen mit Bezug auf die *Verarbeitung* sind innerhalb von drei (3) Arbeitstagen zu melden.
8. Wird der Auftragnehmer mit Tätigkeiten nach Ziff. III.1. Satz 2 beauftragt (u.a. Nutzungskontrolle, Rechteverwaltung bzw. Zugriffsrechte auf Datenbestände, Programmfunktionen usw.), ist der Auftraggeber gehalten, die Einstellungen und Funktionen unverzüglich zu überprüfen.
9. Weitere Pflichten und Rechte des Auftraggebers ergeben sich aus den Regelungen der *VAV*, der EU-DSGVO sowie den gesetzlichen Bestimmungen.
10. Der Auftraggeber hat neben der Vergütung gemäß dem anwendbaren *Hauptvertrag* den etwa anfallenden Aufwand bzw. die Vergütung für Tätigkeiten des Auftragnehmers zu tragen, für die in der *VAV* eine Kostentragung bzw. Vergütung vereinbart ist.

**V. Grundlegende Pflichten des Auftragnehmers**

1. Der Auftragnehmer hat eigene Pflichten gemäß Art. 28 bis 33 EU-DSGVO, im Einzelnen:
a) Er gewährleistet und kontrolliert regelmäßig, dass die auftragsgemäße Verarbeitung nach dem *Hauptvertrag* im jeweils eigenen Verantwortungsbereich (einschl. jeweiliger Unterauftragnehmer), in Übereinstimmung mit den Bestimmungen der *VAV* und der gesetzlichen Vorschriften erfolgt.
b) Er dokumentiert jede ausgeführte Leistung und übermittelt diese unverzüglich dem Auftraggeber.
c) Er hat einen *Datenschutzbeauftragten (DSB)* bestellt, dessen Kontaktdaten unter **https://www.wizard.de** hinterlegt sind.
d) Er darf ohne vorherige dokumentierte Zustimmung des Auftraggebers keine Kopien oder Duplikate der *Auftraggeber-Daten* anfertigen. Hiervon ausgenommen sind Kopien, die zur Gewährleistung einer ordnungsgemäßen *Verarbeitung* und zur ordnungsgemäßen Erbringung der Leistungen gemäß dem jeweiligen *Hauptvertrag*, z.B. einer vereinbarten Datensicherung, erforderlich sind, sowie Kopien, die zur Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
e) Er unterstützt den Auftraggeber bei Kontrollen durch die Aufsichtsbehörde im Rahmen des Zumutbaren und Erforderlichen, soweit diese Kontrollen die *Auftragsverarbeitung* betreffen. Den hierbei entstehenden Aufwand trägt der Auftraggeber.
f) Er hat dem Auftraggeber auf Anforderung eine Übersicht über die in Art. 30 Abs. 2 EU-DSGVO genannten Angaben auszuhändigen.
g) Er setzt zur Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, Art. 29, Art. 32 Abs. 4 EU-DSGVO bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Personen aufseiten des Auftragnehmers, die Zugang zu *Auftraggeber-Daten* haben, dürfen diese ausschließlich entsprechend der Weisung des Auftraggebers und dieser *VAV* verarbeiten, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
h) Er gewährleistet die Umsetzung und Einhaltung der vereinbarten *TOM*, soweit er nach II 3. zuständig ist.
i) Die Vertragspartner arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen. Hierzu leistet der Auftragnehmer die notwendigen Beiträge. Hierdurch entstehenden Aufwand hat der Auftraggeber zu tragen.
j) Er hat den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde zu informieren, soweit sie sich auf die *Auftragsverarbeitung* beziehen. Dies gilt auch - solange das rechtlich zulässig ist - wenn eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die *Auftragsverarbeitung* beim Auftragnehmer ermittelt.
k) Soweit der Auftraggeber einer Kontrolle der Aufsichtsbehörde, 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, hat ihn dieser nach besten Kräften zu unterstützen. Den hierbei entstehenden Aufwand trägt der Auftraggeber.
l) Tätigkeiten, die der Verantwortliche schuldet, z.B. Löschkonzepte, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft sind nur dann und insoweit unmittelbar durch den Auftragnehmer durchzuführen, als sie gemäß dem jeweiligen Hauptvertrag vom Leistungsumfang umfasst sind.
2. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung von dessen in Art. 32 bis 36 EU-DSGVO genannten Pflichten zur Sicherheit von personenbezogenen Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherigen Konsultationen.
Zu den Pflichten gehören für die *Auftragsverarbeitung* u.a.
a) die Sicherstellung eines angemessenen Schutzniveaus durch die *TOM*, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen,
b) die Verpflichtung, Verletzungen von Auftraggeber-Daten unverzüglich an den Auftraggeber zu melden,
c) die Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht gegenüber betroffenen Personen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen,
d) die Unterstützung des Auftraggebers für eine von diesem etwa vorzunehmende Datenschutz-Folgenabschätzung,
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.
Sofern und soweit die Leistungen und Tätigkeiten nicht in der Leistungsbeschreibung gemäß dem anwendbaren *Hauptvertrag* enthalten sind oder der Auftraggeber nachweist, dass sie auf ein Verschulden des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer für die nach Ziff. 2 anfallenden Tätigkeiten eine gesonderte Vergütung beanspruchen.
3. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er feststellt, dass er oder ein Mitarbeiter bei der *Auftragsverarbeitung* gegen datenschutzrechtliche Vorschriften oder gegen Festlegungen aus der *VAV* oder dem anwendbaren *Hauptvertrag* verstoßen hat/haben, sofern und soweit deshalb die Gefahr besteht, dass Auftraggeber-Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind.
4. Ist der Auftraggeber Berufsgeheimnisträger i.S.d. § 203 StGB (dies sind u.a. Steuerberater, Wirtschaftsprüfer, Rechtsanwälte, Notare, Ärzte usw.), wirkt WIZARD als Auftragnehmer in der Eigenschaft als IT-Dienstleister zum Teil an der beruflichen Tätigkeit des Auftraggebers i.S.d. § 203 Abs. 3 Satz 2 StGB mit. Mitarbeiter und Subunternehmer von WIZARD sind in diesem Sinne weitere Mitwirkende nach § 203 Abs. 3 Satz 3 StGB. Für diesen Fall gelten zusätzlich die nachstehenden Verpflichtungen:
a) WIZARD wahrt als Auftragnehmer in Kenntnis der strafrechtlichen Folgen einer Verletzung der Verschwiegenheitspflicht gemäß § 203 StGB (Freiheitsstrafe bis zu einem Jahr oder Geldstrafe) und den sonst anwendbaren rechtlichen Vorschriften fremde Geheimnisse, die WIZARD als Auftragnehmer von dem Auftraggeber zugänglich gemacht werden.
b) WIZARD verpflichtet sich als Auftragnehmer, sich nur insoweit Kenntnis von fremden Geheimnissen im Sinne der vorstehenden Position zu verschaffen, als dies zur Erfüllung eines Hauptvertrags erforderlich ist.
c) WIZARD als Auftragnehmer ist bekannt, dass sich die Verschwiegenheitspflicht nicht nur auf fremde Geheimnisse erstreckt, sondern auf alle Tatsachen, die in Ausübung oder aus Anlass der Tätigkeit für den Auftraggeber, der einer beruflichen Verschwiegenheitsverpflichtung unterliegt, anvertraut oder bekannt werden. Hierzu gehört auch schon die Kenntnis, welche Mandate betreut werden.
d) Bei der Inanspruchnahme von Leistungen, die unmittelbar einem einzelnen Mandat oder einer einzelnen Person dienen, ist der Auftraggeber verpflichtet, die Einwilligung des Mandanten in die Zugänglichmachung von fremden Geheimnissen i.S.v. Ziff. 3 einzuholen.
e) Die vorstehend vereinbarte Pflicht zur Verschwiegenheit besteht nicht, soweit WIZARD auf Grund einer behördlichen oder gerichtlichen Entscheidung zur Offenlegung von vertraulichen Informationen des Auftraggebers verpflichtet ist/wurde. Soweit dies im Einzelfall zulässig und möglich ist, wird WIZARD den Auftraggeber über die Pflicht zur Offenlegung möglichst vorab in Kenntnis setzen.
f) WIZARD ist die Rechtslage zu §§ 53a i.V.m. 53, 97 StPO, §§ 383 f ZPO bekannt (Mitwirkung an der beruflichen Tätigkeit eines Auftraggebers, der einer beruflichen Verschwiegenheitsverpflichtung unterliegt). Der o.a. Kreis von Beteiligten wird bei Gerichten und Behörden über Tatsachen, die mit der Tätigkeit bekannt werden, ohne vorherige Genehmigung des Auftraggebers nicht aussagen oder sonst Auskunft erteilen.

**VI. Technische und organisatorische Maßnahmen (TOM)**

1. Der Auftragnehmer gewährleistet die für die *Auftragsverarbeitung* notwendige Sicherheit der *Verarbeitung* gem. Art. 28 Abs. 3 lit. c, Art. 32 EU-DSGVO, indem er folgende Verpflichtungen übernimmt:
a) Implementierung der unter **www.wizard.de** einsehbaren *TOM* vor Aufnahme der *Auftragsverarbeitung*,
b) Aufrechterhaltung der *TOM* über die Laufzeit der *Auftragsverarbeitung* einschl. einer etwa nachlaufenden Verpflichtung gemäß Ziffer IV.8,
c) Kontrolle der Einhaltung der *TOM* in den gemäß den *TOM* geltenden Zyklen,
d) unverzügliche Nachsteuerung bei Abweichungen vom Sollzustand bei den *TOM*,
e) Kontrolle der Umsetzung der Nachsteuerung sowie
f) Dokumentation der in diesem Rahmen durchgeführten Tätigkeiten einschließlich der dabei gehandhabten Prozesse.
2. Der Auftraggeber informiert sich vor Abschluss der *VAV* und während der Gültigkeit der *VAV* regelmäßig über die *TOM*. Er trägt die Verantwortung dafür, dass die jeweils geltenden *TOM* für die Risiken der zu *verarbeitenden* Daten ein angemessenes Schutzniveau bieten.
3. Da die *TOM* dem technischen Fortschritt unterliegen, ist es dem Auftragnehmer gestattet, auf eigene Kosten abweichende *TOM* umzusetzen, sofern dabei das Sicherheitsniveau der zuvor festgelegten *TOM* nicht unterschritten wird. Die abweichenden *TOM* werden dokumentiert und dem Auftraggeber mitgeteilt, insbesondere wenn es nach einer stattgefundenen Datenschutz-Folgeabschätzung zu einer Neubewertung der geltenden TOM kommt.

**VII. Kontrollrechte des Auftraggebers**

1. Der Auftraggeber ist berechtigt, innerhalb der im anwendbaren *Hauptvertrag* vereinbarten Geschäftszeiten des Auftragnehmers, montags bis freitags zwischen 9:00 und 18:00 Uhr, auf eigene Kosten, ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragnehmers, die Geschäftsräume des Auftragnehmers in denen *Auftraggeber-Daten verarbeitet* werden, zu betreten, um sich im gesetzlichen Rahmen von der Einhaltung der *TOM* und der Ordnungsgemäßheit der *Verarbeitung* zu überzeugen sowie die mit den *TOM* und der Ordnungsgemäßheit der *Verarbeitung* in Zusammenhang stehenden Unterlagen einzusehen (Kontrolle).
2. Sofern nicht anderweitig vereinbart, erfolgt eine Kontrolle durch den beruflich oder gesetzlich bzw. nach Maßgabe von Ziffer V.4 zur Verschwiegenheit verpflichteten *DSB* des Auftraggebers.
3. Der Auftragnehmer gewährt dem Auftraggeber bzw. dessen *DSB* oder Prüfer die zur Durchführung der Kontrolle erforderlichen Zugangs-, Auskunfts- und Einsichtsrechte. Eine Vor-Ort-Kontrolle ist grundsätzlich als Stichprobenkontrolle der für die Durchführung der *Auftragsverarbeitung* relevanten Bereiche auszugestalten.
4. Der Auftragnehmer ist – nach eigenem Ermessen, jedoch unter Berücksichtigung bestehender gesetzlicher Verpflichtungen des Auftraggebers – berechtigt, im Rahmen von Prüfungen und Kontrollen solche Informationen nicht zu offenbaren, die Betriebsgeheimnisse des Auftragnehmers enthalten (z.B. Informationen zu Kosten, Qualitätsprüfungs- und Vertrags-Managementberichte) oder durch deren Offenbarung der Auftragnehmer gegen gesetzliche oder Verpflichtungen aus Verträgen mit Dritten (z.B. Daten anderer Kunden) verstoßen würde.
5. Der Auftraggeber hat den Auftragnehmer rechtzeitig - i.d.R. mindestens vier (4) Wochen vorher - über alle mit der Durchführung der Kontrolle zusammenhängenden Umstände in Textform zu informieren und den Prüfungsumfang im Vorhinein zu dokumentieren. Der Auftraggeber darf in der Regel eine Kontrolle pro Kalenderjahr durchführen lassen, sofern nicht im *Hauptvertrag* weitere Kontrollen vereinbart sind. Hiervon unbenommen ist das Recht des Auftraggebers, weitere Kontrollen durchzuführen, wenn er Kenntnis von sicherheitsrelevanten Vorgängen mit möglichen Auswirkungen auf Auftraggeber-Daten erlangt.
6. Der Auftraggeber hat den *DSB* bzw. Prüfer schriftlich ebenso zu verpflichten, wie der Auftraggeber selbst aufgrund von dieser Ziffer VII. gegenüber dem Auftragnehmer verpflichtet ist. Zudem hat der Auftraggeber den Prüfer auf Verschwiegenheit und Geheimhaltung zu verpflichten. Auf Verlangen des Auftragnehmers hat der Auftraggeber diesem die Verpflichtungsvereinbarungen unverzüglich vorzulegen.

Der Auftraggeber darf keinen Konkurrenten des Auftragnehmers mit der Kontrolle beauftragen.
7. Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der *TOM* anstatt einer Vor-Ort-Kontrolle auch
a) durch die Vorlage eines geeigneten, aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, externe Datenschutz-Auditoren oder Qualitäts-Auditoren);
b) durch eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutz-Auditoren erbracht werden, wenn die entsprechenden Dokumente es dem Auftraggeber in angemessener Weise ermöglichen, sich von der Einhaltung der *TOM* zu überzeugen.
8. Der Auftragnehmer erhält vom Auftraggeber eine Kostenerstattung entsprechend dem aufgewendeten Aufwand in Höhe von 120 € / pro Stunde.

**VIII. Unterauftragsverhältnisse**

1. Als Unterauftragsverhältnisse sind Leistungen eines weiteren Auftragsverarbeiters anzusehen, die sich unmittelbar auf die Erbringung einer Hauptleistung gemäß dem anwendbaren *Hauptvertrag* oder der *VAV* beziehen. Nicht hierzu gehören i.d.R. Nebenleistungen, die z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen durch Dritte erbracht werden; zur Gewährleistung des Datenschutzes und der Datensicherheit der Auftraggeber-Daten sind vonseiten des Auftragnehmers auch bei solchen ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
2. Der Auftraggeber erteilt hiermit die Genehmigung, weitere Auftragsverarbeiter i.S.d. Art. 28 EU-DSGVO in Anspruch zu nehmen. Die jeweils aktuell eingesetzten, weiteren Auftragsverarbeiter mit den für sie jeweils einschlägigen Arbeitsbereichen/Tätigkeiten kann der Auftraggeber unter **www.wizard.de** im Dokument **„Unterauftragsverhältnisse“** abrufen. Weiteren Auftragsverarbeitern sind die datenschutzrechtlichen Pflichten aus der *VAV* ebenfalls aufzuerlegen; dies ist Voraussetzung für ihre Einschaltung.
3. Der Auftraggeber wird in Textform vom Auftragnehmer informiert, wenn eine Änderung in Bezug auf die Hinzuziehung oder die Ersetzung der weiteren Auftragsverarbeiter oder eine sonstige Änderung im Bereich der weiteren Auftragsverarbeiter beabsichtigt ist. Die beabsichtigten Änderungen kann der Auftraggeber unter **www.wizard.de** im Dokument **„Unterauftragsverhältnisse“** abrufen.
Der Auftraggeber kann Einspruch gegen die beabsichtigte Änderung innerhalb von 4 (vier) Wochen nach Zugang der Information über die Änderung in Textform erheben.
4. Ein Einspruch darf vom Auftraggeber nur aus wichtigem Grund ausgesprochen werden.
5. Im Fall des wirksamen Einspruchs kann der Auftragnehmer nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder - sofern ihm die Erbringung der Leistung ohne die beabsichtigte Änderung nicht möglich oder nicht zumutbar ist - die von der Änderung betroffene Leistung gegenüber dem Auftraggeber innerhalb von 4 (vier) Wochen nach Zugang des Einspruchs kündigen.

**IX. Rechte der betroffenen Personen**

1. Betroffene Personen können grundsätzlich ihre Rechte, insbesondere solche gem. Kapitel III der EU-DSGVO, nur gegenüber dem Auftraggeber als Verantwortlichem geltend machen. Wenn sich eine betroffene Person unmittelbar an den Auftragnehmer zwecks Auskunft, Berichtigung, Löschung oder Einschränkung der *Verarbeitung* ihrer *personenbezogenen Daten* wenden sollte, wird dieses Ersuchen unverzüglich an den Auftraggeber weiter geleitet, soweit nicht ein Fall von Ziff. V. 1. l) vorliegt.
2. Der Auftragnehmer unterstützt unter Berücksichtigung der Art der *Verarbeitung* und der ihm zur Verfügung stehenden Informationen den Auftraggeber bei der Einhaltung seiner Pflichten nach Kapitel III. EU-DSGVO gegenüber der betroffenen Person. Der Auftragnehmer wird es dem Auftraggeber durch entsprechende Maßnahmen nach jeweiliger Leistungsbeschreibung ermöglichen, Auftraggeber-Daten zu berichtigen, zu löschen oder die *Verarbeitung* einzuschränken oder auf dokumentiertes Verlangen des Auftraggebers hin die Berichtigung, Einschränkung der *Verarbeitung* oder Löschung vornehmen, wenn und soweit das dem Auftraggeber selbst technisch oder fachlich nicht möglich ist oder er dies gesondert beauftragt.
3. Der Auftragnehmer ist berechtigt, für diese Leistungen eine angemessene gesonderte Vergütung vom Auftraggeber zu verlangen, sofern nicht ein Fall von Ziff. V. 1. l) vorliegt und diese Leistungen in der Leistungsbeschreibung oder anderweitig im *Hauptvertrag* bepreist sind.

**X. Rückgabe und Löschung von Auftraggeber-Daten bzw. Datenträgern im WIZARD-Rechenzentrum**

1. Nach Abschluss der Erbringung der Leistungen zur *Verarbeitung* gemäß dem anwendbaren *Hauptvertrag* führt der Auftragnehmer nach Vorgabe des Auftraggebers folgenden Tätigkeiten aus:
Er gibt diese in einem gängigen, im Zweifel dem für die Verarbeitung der Auftraggeber-Daten verwendeten Format an einen nachfolgenden Auftragsverarbeiter oder Dritten heraus (gem. Art. 20 Abs. 2 EU-DSGVO und bei Vorliegen der Voraussetzungen des Art. 20 EU-DSGVO).
Die Verpflichtung zur Löschung bzw. Übergabe gilt sofern nicht nach dem Recht der Europäischen Union oder nach deutschem Recht eine Verpflichtung zur Speicherung der Auftraggeber-Daten besteht oder sich aus dem *Hauptvertrag* etwas anderes ergibt.
3. Vorbehaltlich abweichender Vereinbarung werden bei Vertragsende die Auftraggeber-Daten auf einem vom Auftraggeber zuvor bereitgestellten Datenträger in dem für die *Verarbeitung* der Auftraggeber-Daten verwendeten Format an diesen übergeben und beim Auftragnehmer gelöscht. Der Auftragnehmer wird ansonsten die Löschung innerhalb von neunzig (90) Tagen vornehmen.
4. Der Aufwand für die Herstellung des Datenabzugs, sowie, falls gewünscht, die zusätzlichen Kurier- bzw. Transportkosten und ggfs. die Kosten eines Datenträgers, werden dem Auftraggeber gesondert in Rechnung gestellt.
5. Tätigkeiten zur Außerbetriebnahme, Datenübergabe bzw. Löschung erfolgen innerhalb der Servicezeiten, arbeitstäglich montags bis freitags zwischen 9:00 und 18:00 Uhr.
6. Betriebssystem-Images, Programme, System- und Konfigurationsdateien werden nicht mit übergeben. Die Systemumgebung und die aktiven Speicherbereiche des Auftraggebers werden zum Vertragsende gelöscht.
7. Sofern ein *Hauptvertrag* aus wichtigem Grund ganz oder teilweise fristlos oder sonst vorzeitig gekündigt oder auf andere Weise mit einer Frist von weniger als einer (1) Woche vorzeitig beendet wird, erhält der Auftraggeber die Gelegenheit, die von der (Teil-) Kündigung bzw. Beendigung betroffenen Auftraggeber-Daten innerhalb einer Frist von vier (4) Wochen nach rechtlicher Beendigung auf sich oder auf einen von ihm bestimmten Dritten nach Maßgabe von Ziff. 1 überzuleiten. Bewirkt der Auftraggeber eine Überleitung der Auftraggeber-Daten nicht innerhalb der o.a. Frist, d.h., nimmt er eine bestehende technische Möglichkeit der Überleitung innerhalb der Frist nicht wahr, ist der Auftragnehmer berechtigt, die Auftraggeber-Daten zu löschen.
8. Sofern Leistung gemäß dem *Hauptvertrag* eine Datenaufbewahrung ist, z.B. eine Archivierung, insbesondere über die Laufzeit einer *Verarbeitungstätigkeit* hinaus, werden diese Auftraggeber-Daten erst nach Ablauf der vereinbarten Archivierungszeit gelöscht. Wünscht der Auftraggeber eine relativ dazu vorzeitige Löschung, unterbreitet ihm der Auftragnehmer ein Angebot für die Vornahme der Löschungstätigkeit.
9. Dokumentationen, die dem Nachweis der ordnungsgemäßen *Auftragsverarbeitung* dienen, bewahrt der Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus auf.
10. Sofern und soweit sich unter Anwendung der vorstehenden Regelungen auch nach der rechtlichen Beendigung bzw. Teilbeendigung eines *Hauptvertrages* noch von der Beendigung betroffene Auftraggeber-Daten auf Systemen des Auftragnehmers befinden, z.B. in Archiven, gelten die Vorschriften der *VAV* weiter.

**XI. Haftung, Haftungsverteilung, Haftung im Innenverhältnis**

1. Für die Haftung gelten die Regelungen zur Haftung aus dem *Hauptvertrag* entsprechend.
2. Sofern der Auftraggeber aus der EU-DSGVO oder aus anderen datenschutzrechtlichen Vorschriften, insbesondere gegenüber der betroffenen Person oder einer Aufsichtsbehörde, verpflichtet ist, ein EU-DSGVO-konformes Verhalten nachzuweisen, gilt diese Beweislastverteilung auch im Innenverhältnis zum Auftragnehmer.
3. Die datenschutzrechtliche Verantwortung für die *Auftragsverarbeitung* verbleibt in dem gesetzlichen Rahmen beim Auftraggeber, soweit nicht datenschutzrechtliche Vorschriften Verpflichtungen für den Auftragnehmer einer *Auftragsverarbeitung* begründen und der Auftragnehmer diese Verpflichtungen nicht mindestens fahrlässig verletzt. Soweit der Auftraggeber besonderen berufsrechtlichen Vorschriften unterliegt, haftet der Auftraggeber selbst für deren Einhaltung.

**XII. Inkrafttreten, Beendigung, Ablösung bestehender Vereinbarungen**

1. Die *VAV* tritt unmittelbar nach beidseitiger Anerkennung in Kraft.
2. Die *VAV* löst eine ggfs. bestehende alte Vereinbarung zur Auftragsdatenverarbeitung nach § 11 BDSG der Vertragspartner nahtlos ab. Die Vertragspartner sind sich darüber einig, dass zwischen der *VAV* und einer etwa bestehenden bisherigen Vereinbarung zeitlich keine Lücke mit Blick auf die *Auftragsverarbeitung* bzw. Auftragsdatenverarbeitung besteht.
3. Etwa aus dem Zeitraum der Geltung der abgelösten Vereinbarung noch offene Ansprüche, z.B. auf Schadensersatz, werden nach der abgelösten Vereinbarung behandelt. Alle datenschutzrechtlich relevanten Ereignisse, die ab dem Inkrafttreten dieser neuen *VAV* stattfinden, werden unter der *VAV* behandelt.
4. Laufzeit und Kündigung der *VAV* richten sich im Übrigen nach den Bestimmungen zur Laufzeit und Kündigung der von der *VAV* erfassten Hauptverträge. Eine auf Beendigung eines einzelnen *Hauptvertrags* gerichtete wirksame Erklärung, gleich wann und aus welchem Grund, bewirkt ohne gesonderte Erklärung auch eine Kündigung der *VAV* auf denselben Zeitpunkt, bezogen jedoch nur auf den jeweils gekündigten *Hauptvertrag*. Eine Beendigung der *VAV* im Ganzen erfolgt vorbehaltlich abweichender Regelungen in Ziff. X insoweit nur mit der Beendigung des zeitlich letzten *Hauptvertrages*. Eine isolierte Kündigung der *VAV* ist ausgeschlossen.

**XIII. Verhältnis zum Hauptvertrag**

1. Soweit in der *VAV* keine Sonderregelungen enthalten sind, gilt der *Hauptvertrag*.
2. Im Fall von Widersprüchen zwischen der *VAV* einerseits und Regelungen aus sonstigen Vereinbarungen der Vertragspartner, insbesondere aus einem *Hauptvertrag* andererseits, gehen die Regelungen aus der *VAV* immer vor.

**XIV. Schlussbestimmungen**

1. Mündliche Nebenabreden werden nicht Vertragsbestandteil. Änderungen und Ergänzungen bedürfen der Textform (§ 126b BGB).
2. Auf das Rechtsverhältnis der Vertragspartner findet ausschließlich das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts und des Kollisionsrechts Anwendung.
3. Ausschließlicher, auch internationaler Gerichtsstand für alle sich aus dieser Vereinbarung unmittelbar oder mittelbar ergebenden Streitigkeiten ist das für den Sitz von WIZARD zuständige Landgericht. Diese Gerichtsstandsvereinbarung findet keine Anwendung, wenn die Streitigkeit andere als vermögensrechtliche Ansprüche betrifft oder für die Streitigkeit bereits nach den gesetzlichen Bestimmungen ein ausschließlicher Gerichtsstand begründet wird.
4. Sollte eine der Bestimmungen der *VAV* oder eine mit Bezug hierauf geschlossene weitere Vereinbarung, gleich wann und aus welchem Grund, unwirksam sein oder werden, oder die *VAV* eine nach übereinstimmender Auffassung der Vertragspartner regelungsbedürftige Lücke enthalten, berührt dies die Wirksamkeit der übrigen Bestimmungen nicht. Die Vertragspartner werden in einem solchen Fall versuchen, die unwirksame oder lückenhafte Bestimmung durch eine neue Bestimmung zu ersetzen, die der unwirksamen oder lückenhaften Bestimmung nach dem Willen der Vertragspartner im Zeitpunkt der Unterzeichnung dieser Vereinbarung wirtschaftlich am Nächsten kommt. Bis zu einer solchen Ersetzung gelten anstelle der unwirksamen oder lückenhaften Bestimmung die gesetzlichen Regelungen.

*Auftragnehmer:*

Bremervörde, den_____

_____
WIZARD Computersyteme GmbH

*Auftraggeber:*

_____, den_____

_____
Unterschrift Auftraggeber