Vertrag zur Auftragsverarbeitung

gemäß Art. 28 EU-DSGVO

DOKUMENTENEIGENSCHAFTEN	
Titel	Auftragsdatenvereinbarung
Betreff	Auftragsdatenvereinbarung
Autor	RA WAGNER, WOLFF GÖBEL WAGNER
Dokumentendatum	04.05.2018

ÄNDERUNGSEINTRAG		
Datum	**Autor**	**Änderung**
04.05.2018	Jennifer Hülskötter	Anpassungen an Hülskötter & Partner Consulting und Vertriebs GmbH
11.03.2020	Jennifer Hülskötter	Anpassung der TOMs in Anlage 1
06.09.2022	Monique Boje	Anpassung an Hülskötter & Partner Consulting und Vertriebs GmbH
12.10.2022	Monique Boje	Anpassung der Subunternehmer in Anlage 2

zwischen

*- nachfolgend „**Auftraggeber**" -*

und

Hülskötter & Partner Consulting und Vertriebs GmbH
An den Bahngleisen 10
48356 Nordwalde

*- nachfolgend „**Auftragnehmer**" -*

*- nachfolgend Auftraggeber und Auftragnehmer gemeinsam als „**Parteien**" bezeichnet -*

PRÄAMBEL

Der Auftraggeber möchte den Auftragnehmer mit den in § 3 genannten Leistungen beauftragen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DS-GVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung, deren Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

§ 1 BEGRIFFSBESTIMMUNGEN

(1) Verantwortlicher ist gem. Art. 4 Abs. 7 DS-GVO die Stelle, die alleine oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(2) Auftragsverarbeiter ist gem. Art. 4 Abs. 8 DS-GVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

(3) Personenbezogene Daten sind gem. Art. 4 Abs. 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) 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, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

(4) Besonders schutzbedürftige personenbezogene Daten sind personenbezogenen Daten gem. Art. 9 DS-GVO, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit von Betroffenen hervorgehen, personenbezogene Daten gem. Art. 10 DS-GVO über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln sowie genetische Daten gem. Art. 4 Abs. 13 DS-GVO, biometrischen Daten gem. Art. 4 Abs. 14 DS-GVO, Gesundheitsdaten gem. Art. 4 Abs. 15 DS-GVO sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

(5) Verarbeitung ist gem. Art. 4 Abs. 2 DS-GVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(6) Aufsichtsbehörde ist gem. Art. 4 Abs. 21 DS-GVO eine von einem Mitgliedstaat gem. Art. 51 DS-GVO eingerichtete unabhängige staatliche Stelle.

§ 2 ANGABE DER ZUSTÄNDIGEN DATENSCHUTZ-AUFSICHTSBEHÖRDE

(1) Zuständige Aufsichtsbehörde für den Auftraggeber ist: Sachsen-Anhalt

(2) Zuständige Aufsichtsbehörde für den Auftragnehmer ist Nordrhein-Westfalen.

(3) Der Auftraggeber und der Auftragnehmer und gegebenenfalls deren Vertreter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

§ 3 VERTRAGSGEGENSTAND

(1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich Softwaresupport, IT-Dienstleistungen, Schulungen im Bereich Kanzleiorganisation und Hosting. Grundlage ist die aktuellste Version des Softwarepflege- oder Hostingvertrages des Auftraggebers („Hauptvertrag“). Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers. Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus dem Hauptvertrag (und der dazugehörigen Leistungsbeschreibung sowie den Anlagen des Hauptvertrages). Dem Auftraggeber obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.

(2) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

(3) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden.

(4) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

§ 4 WEISUNGSRECHT

(1) Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers erheben, verarbeiten oder nutzen; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

(2) Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten.

(3) Die weisungsberechtigten Personen beim Auftragnehmer: Mitarbeiter in den Bereichen Support und Technik.

(4) Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen ist dem Vertragspartner unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen.

(5) Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

(6) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 5 ART DER VERARBEITETEN DATEN, KREIS DER BETROFFENEN

(1) Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragnehmer Zugriff auf personenbezogenen Daten:
   a. Name und Anschrift
   b. Finanzdaten
   c. Telefonnummer und E-Mail-Adresse

(2) Diese Daten umfassen unter Umstände folgende besonderen Kategorien personenbezogener Daten:
   a. Gewerkschaftszugehörigkeit der Mandanten von Anwaltskanzleien
   b. Rassische- und ethnische Herkunft der Mandanten von Anwaltskanzleien
   c. Bonitätsauskunft von Mandanten von Anwaltskanzleien

(3) Der Kreis der von der Datenverarbeitung Betroffenen:
   a. Mandanten- und Beteiligtendaten von Anwaltskanzleien
   b. Mitarbeiterdaten von Anwaltskanzleien

§ 6 SCHUTZMASSNAHMEN DES AUFTRAGNEHMERS

(1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DS-GVO, insbesondere mindestens die in Anlage 1 aufgeführten Maßnahmen der

a. Zutrittskontrolle
b. Zugangskontrolle
c. Zugriffskontrolle
d. Trennungskontrolle
e. Pseudonymisierung
f. Weitergabekontrolle
g. Eingabekontrolle
h. Auftragskontrolle
i. Verfügbarkeitskontrolle
j. Datenschutz Maßnahmen
k. Incident-Response Management

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Beim Auftragnehmer ist als Ansprechpartner für den Datenschutz Herr Olaf Tenti bestellt:

GDI Gesellschaft für Datenschutz und Informationssicherheit mbH

Körnerstraße 45
58095 Hagen
Tel: +49-2331-356 832-0
Fax: +49-2331-356 832-1
E-Mail: info@gdi-mbh.eu

(4) Der Auftragnehmer veröffentlicht die Kontaktdaten des Datenschutzbeauftragten auf seiner Internetseite und teilt sie der Aufsichtsbehörde mit. Veröffentlichung und Mitteilung weist der Auftragnehmer auf Anforderung des Auftraggebers in geeigneter Weise nach.

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

(6) Der Auftragnehmer darf seinen Beschäftigten, die mit der Verarbeitung von personenbezogenen Daten für den Auftraggeber beauftragt sind, pandemiebedingt in Ausnahmefällen die Verarbeitung von personenbezogenen Daten in Privatwohnungen („Home-Office“) unter Einhaltung der nachfolgenden Regelungen erlauben, gleiches gilt für Beschäftigte, die mobil arbeiten:
Der Auftragnehmer hat sicherzustellen, dass die Einhaltung der vertraglich vereinbarten technischen und organisatorischen Maßnahmen auch im „Home-Office“ der Beschäftigten des Auftragnehmers gewährleistet ist. Der Auftragnehmer trägt insbesondere Sorge dafür, dass bei einer Verarbeitung von personenbezogen 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.
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.
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 zu treffenden Maßnahmen erfolgt.

§ 7 INFORMATIONSPFLICHTEN DES AUFTRAGNEHMERS

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder Textform informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:
   a. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;
   b. eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(2) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den Auftraggeber und ersucht um weitere Weisungen.

(3) Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.

(4) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der DS-GVO liegen.

(5) Über wesentliche Änderung der Sicherheitsmaßnahmen nach § 6 Abs. 2 hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten.

(6) Ein Wechsel in der Person des betrieblichen Datenschutzbeauftragten/Ansprechpartners für den Datenschutz ist dem Auftraggeber unverzüglich mitzuteilen.

(7) Der Auftragnehmer und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DS-GVO enthält. Das Verzeichnis ist dem Auftraggeber auf Anforderung zur Verfügung zu stellen.

(8) An der Erstellung des Verfahrensverzeichnisses durch den Auftraggeber hat der Auftragnehmer im angemessenen Umfang mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

§ 8 KONTROLLRECHTE DES AUFTRAGGEBERS

(1) Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig in angemessenen Abständen von den technischen und organisatorischen Maßnahmen des Auftragnehmers.

Hierfür kann er z. B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind.

(3) Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

(4) Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung.

(5) Der Auftragnehmer weist dem Auftraggeber die Verpflichtung der Mitarbeiter nach § 6 Abs. 4 auf Verlangen nach.

§ 9 EINSATZ VON SUBUNTERNEHMERN

(1) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in Anlage 2 genannten Subunternehmer durchgeführt. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt. Der Auftragnehmer ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) direkt gegenüber den Subunternehmern wahrnehmen kann. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

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

§ 10 ANFRAGEN UND RECHTE BETROFFENER

(1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32 bis 36 DS-GVO.

(2) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

§ 11 HAFTUNG

(1) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragnehmer alleine der Auftraggeber gegenüber dem Betroffenen verantwortlich.

(2) Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.

§ 12 AUSSERORDENTLICHES KÜNDIGUNGSRECHT

Der Auftraggeber kann den Hauptvertrag fristlos ganz oder teilweise kündigen, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DS-GVO vorsätzlich oder grob fahrlässig verletzt oder eine Weisung des Auftraggebers nicht ausführen kann oder will. Bei einfachen – also weder vorsätzlichen noch grob fahrlässigen – Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist, innerhalb welcher der Auftragnehmer den Verstoß abstellen kann.

§ 13 BEENDIGUNG DES HAUPTVERTRAGS

(1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen. Zu entsorgende Unterlagen sind mit einem Aktenvernichter nach DIN 32757-1 zu vernichten. Zu entsorgende Datenträger sind nach DIN 66399 zu vernichten.

(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren.

(3) Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

§ 14 SCHLUSSBESTIMMUNGEN

(1) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB und/ oder Vermieterpfandrecht hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

(3) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

(4) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist HRB 2039 – Amtsgericht Steinfurt

Folgende ANLAGEN sind vertragsgegenständlich:

ANLAGE 1 – Technische und organisatorische Maßnahmen des Auftragnehmers
ANLAGE 2 – Subunternehmer

Ort, **(Auftraggeber)**	**Nordwalde,** **(Auftragnehmer)**
Unterschrift (Auftraggeber)	**Unterschrift (Auftragnehmer)**
Funktion (Auftraggeber)	**Geschäftsführer** **Funktion (Auftragnehmer)**

Anlage 1

Technische und organisatorische Maßnahmen des Auftragnehmers

1. Zutrittskontrolle

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

Kurzübersicht zu den getroffenen Maßnahmen zur Zutrittskontrolle:

Technische Maßnahmen	Organisatorische Maßnahmen
Alarmanlage	Schlüsselregelung/Liste
Zugangskontrollsystem	Protokollierung von Besuchern über den Kalender
Chipkarten/Transpondersysteme	Besucher in Begleitung durch den Mitarbeiter
Manuelles Schließsystem	Sorgfalt bei der Auswahl der Reinigungsdienste
Sicherheitsschlösser	

Das Unternehmen ist *Eigentümer des Gebäudes*. Innerhalb des Gebäudes befinden sich *keine weiteren Mieter*. Zutritt zum Gebäude haben folglich nur die eigenen Mitarbeiter. Innerhalb des Gebäudes werden *Token und Schlüssel als Schließsysteme* eingesetzt. Die *Schlüsselvergabe ist selektiv* und orientiert sich an den Aufgaben der einzelnen Mitarbeiter. Bei Verlust eines Schlüssels werden nach Meldung alle zugehörigen Schlüssel im Unternehmen ausgetauscht. Die Schließsysteme haben zudem *Sicherheitsschlösser*.

Das Gebäude des Unternehmens ist mit einer *Alarmanlage ausgestattet*. Diese Alarmanlage hat eine direkte Verbindung zum Wachschutz. Der Wachschutz setzt sich bei Alarm mit der Polizei in Verbindung. *Bewegungsmelder* für die Anlage sind innerhalb des gesamten Gebäudes installiert.

Es gibt einen *zentralen Empfangsbereich* für Besucher. Der Besuch wird *durch Klingeln Eintritt gewährt* und am Empfang des Unternehmens abgeholt. Besucher werden immer in ein Besprechungszimmer geführt und werden durch den Empfangenden Mitarbeiter begleitet. Besucher werden im Kalender mit Anlass protokolliert. Bzgl. des Umgang mit Besuchern und externen Dienstleistern werden alle Mitarbeiter regelmäßig sensibilisiert.
Für die Umsetzungen der Regelungen der Zutrittskontrolle ist die Geschäftsführung zuständig. Diese führt auch eine *Dokumentation über die ausgegebenen Schlüssel und Token*. Die Ablage der Dokumentation findet in der Personalakte der Mitarbeiter statt.

Im Unternehmen wird ein Datenschutzkonzept schriftlich in der Unternehmensorganisation umgesetzt. Es existiert eine Softwareübersicht. Handbücher der Hardware und Software sind auf dem Server des Unternehmens abgelegt.

2. Zugangskontrolle

Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und -verfahren benutzen:

Kurzübersicht über die ergriffenen Maßnahmen zur Zugangskontrolle:

Technische Maßnahmen	Organisatorische Maßnahmen
Login mit Benutzernamen und Passwort	Verwalten von Benutzerberechtigungen
Endpointsecurity im Rechenzentrum für Juristen	Zentrale Passwortvergabe
Endpointsecurity an den Client-Rechnern im lokalen LAN	Richtlinie für „sicheres Passwort“
Firewall für das lokale LAN und das Rechenzentrum für Juristen	Richtlinie für „Löschen/Vernichten“ von personenbezogenen Daten
Mobile Device Management	Richtlinie „Clean desk“
Einsatz von VPN beim Remote-Zugriffen	Allgemeine Richtlinie Datenschutz und Sicherheit

Verschlüsselung von Datenträgern	Zugangsbeschränkung Serverraum
Sperre externer Schnittstellen (USB)	
Automatische Desktopsperre	
Verschlüsselung von Notebooks/Tablets	
Verschlüsselte Datenspeicherung im Rechenzentrum von Juristen im aktiven Storage, wie auch im Backup	

Der Serverraum des Unternehmens ist im Zugang beschränkt und gesondert gesichert: Zutrittsberechtigt sind über drei Schlüssel die beiden Geschäftsleitungen und der Leiter der IT. Über die Ausgabe der zugehörigen Schlüssel der Schließsysteme werden verschiedenen Berechtigungsgruppen realisiert. Der Serverraum verfügt über eine Klimaanlage, eine Brandüberwachungsanlage und keine wasserführenden Leitungen.
Weiterhin ist der Archivraum des Unternehmens gesondert gesichert und im Zutritt beschränkt.
Alle Türen, hinter denen sich personenbezogene Daten befinden, sind sowohl während der Dienstzeiten, als auch nach der Arbeitszeit beim Verlassen immer verschlossen.
Die Rechner des Unternehmens sind durch Benutzerprofile mit User-ID und Passwort vor unberechtigtem Zugriff geschützt. Alle Nutzerberechtigungen werden nach dem Need-to-Now Prinzip vergeben.
Alle Mitarbeiter sind aufgrund ihrer Qualifikationen mit den Grundlagen des sicheren Umgangs mit Datenverarbeitungssystemen, insbesondere mit der Vergabe von sicheren Passwörtern, vertraut oder in diesem Bereich nachweislich geschult worden. Die Mitarbeiter sind durch das Active Directory dazu verpflichtet, kryptische Passwörter zu verwenden, die wie folgt aufgebaut sind:

- Passwortwechsel alle 90 Tage
- Mindestzeichenlänge 9
- 1 Großbuchstabe
- 1 Sonderzeichen
- 1 Zahl

Alle Benutzerkonten des Unternehmens werden nach dreimaliger, falscher Eingabe der Benutzeridentifizierung automatisch gesperrt. Eine Entsperrung eines Benutzerkontos kann nur manuell von dem IT Administrator vorgenommen werden.
Alle Clients des Unternehmens (außer Clients zur Administration) haben keine Administrations-Rechte.
Alle IT-Geräte sind mit einer Inventarnummer ausgestattet. Gleichzeitig wird eine Dokumentation geführt.

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können:

Kurzübersicht über die ergriffenen Maßnahmen zur Zugriffskontrolle:

Technische Maßnahmen	**Organisatorische Maßnahmen**
Aktenschredder mind. Stufe 3, cross cut	Einsatz Berechtigungskonzepte
Externer Aktenvernichter (DIN 32757)	Minimale Anzahl von Administratoren
Physische Löschung von Datenträgern bei Entsorgung	Verwaltung von Benutzerrechten durch Administratoren
Protokollierung von Zugriffen auf Anwendungen, konkret bei Eingabe, Änderung und Löschung von Daten	Serverraum in der ersten Etage

Der Serverraum des Unternehmens befindet sich in der ersten Etage. Die gesamte Hardware des Unternehmens wird zentral angeschafft, konfiguriert und installiert: Es liegt ein anwenderbezogenes Berechtigungs- und Rechtekonzept vor, dass im Active Directory umgesetzt wird. Die realisierte Berechtigungsstruktur bezieht sich auf das gesamte System des Unternehmens: Die Berechtigungen können auf Dateien, auf Datensätze, auf

Anwendungsprogramme und das Betriebssystem differenziert werden und die Lese-, Schreib-, Änderungs- und Löschrechte einschränken. Es wird sichergestellt, dass jeder Benutzer nur auf die Daten zugreifen kann, zu denen er zugriffsberechtigt ist. Die Rechtevergabe findet durch die Geschäftsführung im Dialog mit dem Administrator statt. Das Berechtigungskonzept, dass sich an den Stellungen der Mitarbeiter orientiert, ist schriftlich festgehalten (Dokumentation über das Active Directory). Verschiedene Zugriffsrechte werden durch vorgefertigte Benutzerprofile zusammengefasst. Weiterhin ist das Berechtigungskonzept programm-technisch in der Anwendung, im Active Directory hinterlegt. Zum Schutz gegen unberechtigten Zugriff im Arbeitsalltag ist bei allen Benutzerkonten durch das Active Directory der Bildschirmschoner zentral aktiviert. Jedes Konto wird nach zehn Minuten der Inaktivität durch eine erneut erforderliche Eingabe des Passwortes gesichert.
Alle USB-Ports der Mitarbeiter Clients und der Laptops sind gesperrt, sodass USB-Sticks, externe Festplatten, Fotokameras etc. nicht von den Mitarbeitern mit dem Unternehmens-Netzwerk in Verbindung gebracht werden können.

Es wird eine Firewall, die von der Geschäftsführung und dem Rechenzentrum des Unternehmens konfiguriert und gewartet wird, sowie ein Virenscanner (Client- und Serverseitig) eingesetzt.
Die durch Akten erhobenen, verarbeiteten oder genutzten personenbezogenen Daten werden in Schränken aufbewahrt. Die Büroräume werden sowohl während der Arbeitszeiten, als auch nach Dienstende beim Verlassen eines Büros abgeschlossen.
Jegliche Hardware-Entsorgung wird durch die IT Abteilung des Unternehmens umgesetzt. Der Inhalt von Festplatten und Datenträger wird zuerst von der IT Abteilung datenschutzkonform gelöscht.

4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben werden getrennt voneinander verarbeitet werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
Trennung von Produktiv- und Testumgebungen	Steuerung über Berechtigungskonzept
Physikalische Trennung von Datenbanken, Datenträgern und Systemumgebungen	Festlegung von Datenbankrechten
Mandantenfähigkeit relevanter Anwendungen	

5. Pseudonymisierung

Verarbeitung von personenbezogenen Daten auf eine Art und Weise, dass ohne Hinzuziehen zusätzlicher Informationen diese nicht mehr spezifisch einer betroffenen Person zugeordnet werden können. Die zusätzlichen Informationen müssen hierbei getrennt von den pseudonymisierten Daten aufbewahrt werden.

Technische Maßnahmen	Organisatorische Maßnahmen
Zuordnungsdaten für die auf der Webeseite pseudonymisiert gespeicherten Zugangsdaten zu unserem Kundensystem sind auf unterschiedlichen Servern gespeichert (Webserver und interner Sever).	

6. Weitergabekontrolle

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

Kurzübersicht über die ergriffenen Maßnahmen zur Weitergabekontrolle:

Technische Maßnahmen	Organisatorische Maßnahmen
Einsatz von VPN	Dokumentation von Datenempfängern
Protokollierung der Zugriffe und Abrufe	Sorgfalt bei der Auswahl von Transportpersonal – und Fahrzeugen
Weitergabe von sensiblen Daten nur über die selbst gehostete Hülskötter-Dateacloud	Schriftliche Verpflichtung der Mitarbeiter zur Verschwiegenheit und Wahrung der Geschäftsgeheimnisse.
Bereitstellung von Daten und Services über verschlüsselte Verbindungen (https)	

Personenbezogene Daten des Unternehmens werden zur Erfüllung der angebotenen Dienstleistungen und zum Nachkommen der gesetzlichen Vorschriften an folgende externe Stellen übermittelt: Krankenkasse, Finanzamt, betroffene Kunden, Interessenten, Sozialversicherung.
Zur Übertragung der Daten wird der Postweg, VPN, Fax oder Mail genutzt. Durch die Sperrung aller USB-Ports der Mitarbeiter können auf diesem Wege keine Daten intern oder extern weitergegeben werden.

7. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind.

Kurzübersicht über die ergriffenen Maßnahmen zur Eingabekontrolle:

Technische Maßnahmen	Organisatorische Maßnahmen
Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
Manuelle Kontrolle der Protokolle bei Bedarf	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen
	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzeptes
	Klare Zuständigkeiten für Löschung

Zur Gewährleistung der Eingabekontrolle sind die vom Softwarehersteller mitgebrachen Log Mechanismen und Transaktionsprotokolle, zur Protokollierung aller Eingaben für alle Anwendungen, vorhanden. Auch die von Windows mitgelieferten Protokolle sind aktiviert. Protokolle und Log-Einträge jeglicher Art werden bei Bedarf ausgewertet.

8. Verfügbarkeitskontrolle

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

Kurzübersicht über die ergriffenen Maßnahmen zur Verfügbarkeitskontrolle:

Technische Maßnahmen	Organisatorische Maßnahmen
Rauchmeldeanalge	Backup & Recovery Konzept (ausformuliert)
Feuerlöscher im Serverraum	Kontrolle der Sicherungsvorgänge
Serverraum klimatisiert	Regelmäßige Tests zur Datenwiederherstellung
Personenbezogene Daten der Kunden ausgelagter im Rechenzentrum für Juristen, welches den modernen Sicherheitsstandards eines Rechenzentrums entspricht.	Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums

USV	Keine sanitären Anschlüsse im oder oberhalb des Serverraums
Schutzsteckdosenleisten im Serverraum	Existens eines Notfallplans
RAID System/Festplattenspiegelung	Getrennte Partition für Betriebssystem und Daten

Die Server von **Hülskötter & Partner Consulting und Vertriebs GmbH** befinden sich in der ersten Etage des Unternehmens. Der Raum ist in die Brandmeldeanlage des Unternehmens integriert. Es existiert eine Klimaanlage. Wasserführende Leitungen sind nicht vorhanden.
Die Daten auf dem Server werden zentral durch die Geschäftsführung, als auch dezentral in einem Rechenzentrum gesichert. Es liegt ein Datensicherungskonzept vor. Auch das Testen einer Wiedereinspielung (täglich) einer Datensicherung ist gewährleistet. Es ist eine Mehrfachsicherung und Rund-Um-Sicherung aller Daten vorhergesehen. Die zentrale Datensicherung über ein Software-Tool umgesetzt. Die Backup-Datenträger sind in Ihrer Aufbewahrung für die Geschäftsführung zugriffsbeschränkt und gesondert gesichert.
Das Unternehmen setzt eine unterbrechungsfreie Stromversorgung für den Serverraum ein. Die unterbrechungsfreie Stromversorgung wird durch die IT Abteilung regelmäßig hinsichtlich ihrer Wirksamkeit getestet. Bei einem Stromausfäll werden alle wichtigen Geräte (Server etc.) automatisch heruntergefahren.
Das Unternehmen verfügt weiterhin über folgende Speichermedien: Diskette, CD-R, CD-RW, DVD, USB.
Es wird ein regelmäßig, automatisiert aktualisierter Virenscanner und eine regelmäßig kritisch überprüfte Firewall eingesetzt. Durch den Virenscanner werden sowohl eingehende als auch ausgehende Mails gescannt. Die Konfiguration der Regeln, den Aufbau und das regelmäßige Testen der Firewall wird von vier internen IT Abteilung übernommen. Der Betrieb der Firewall wird ständig durch den Administrator und das Rechenzentrum überwacht, sodass gewährleistet wird, dass die Firewall ständig zur Verfügung steht. Sicherheitsrelevante Ereignisse werden automatisch protokolliert und direkt nach der automatischen Meldung auf den Clients der IT Abteilung ausgewertet. Für die Firewall vor Ort ist die Geschäftsführung, für die Firewall im Rechenzentrum das Rechenzentrum selber verantwortlich.

9. Auftragskontrolle

Die Auftragskontrolle beschreibt die Verantwortung des Auftragnehmers, die Schutzmaßnahmen anderer Unternehmen an die er Aufträge im Zuge der Auftragsdatenverarbeitung vergibt, genau zu prüfen.
Die Schutzmaßnahmen externer Dienstleister werden durch einen benannten Verantwortlichen regelmäßig auditiert und vor Vertragsunterzeichnung eingehend bezüglich der internen Sicherheits-anforderungen kontrolliert.

10. Datenschutz-Maßnahmen

Technische Maßnahmen	**Organisatorische Maßnahmen**
Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeiten für Mitarbeiter nach Bedarf in einem zentralen Qualitätsmanagementsystem	Externer Datenschutzbeauftragter: Olaf Tenti GDI mbH Körnerstr 45 58095 Hagen
Anderweitiges dokumentiertes Sicherheitskonzept	Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
	Regelmäßige Sensibiliserung der Mitarbeiter
	Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden
	DSFA wird bei Bedarf durchgeführt
	Jährliches Datenschutzaudit

11. Incident-Response Management

Technische Maßnahmen	Organisatorische Maßnahmen
Einsatz von Firewall und regelmäßige Aktualisierung	Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen/Datenschutzpannen
Einsatz von Spamfiltern und regelmäßige Aktualisierung von Blacklisten	Dokumentierter Prozess zum Umgang mit Sicherheitsvorfällen
Einsatz einer professionellen Endpointsecurity	Einbindung von Datenschutzbeauftragten bei Sicherheitsvorfällen
	Dokumentation von Sicherheitsvorfällen und Datenpannen via Ticketsystem
	Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen

Anlage 2

Subunternehmer

NAME	ART DER DIENSTLEISTUNG
Advo-web GmbH **Im Mühlenteich 56** **D-58300 Wetter a.d. Ruhr**	Bereitstellung der Software advoware und Supportdienstleistungen für advoware
Datenübernahme für Rechtsanwälte und Notare **Berliner Straße 37** **D-53604 Bad Honnef**	Datenmigration von fremder Anwaltssoftware zu advoware
Kollmann Informatik GmbH **Brookkehre 34** **D-21029 Hamburg**	Datenmigration von fremder Anwaltssoftware zu advoware
Wortmann AG **Bredenhop 20** **D-32609 Hüllhorst** **WEEE-Reg.-Nr. DE26723592**	Hosting des Rechenzentrums für Juristen 2.0 Die aktuellen ADV und TOMs der Wortmann AG finden Sie auf der folgenden Seite: https://www.wortmann.de/de-de/content/neu-datenschutz/datenschutz.aspx
Mindtime Backup **Baustraße 4** **D-46446 Emmerich a. Rhein**	Bereitstellung der Software und IT-Infrastruktur von advozon Datensicherung sowie deren 2nd-Level-Support
Prianto GmbH **Barthstraße 18** **D-80339 München**	Bereitstellung der Software von advozon IT-Schutz sowie 2nd-Level-Support
egs computer Vertrieb GmbH **Steinhof 5A** **D-40699 Erkrath**	Lieferant der Software von Nuance - Dragon Naturally Speaking
Nuance, München **Willy-Brandt-Platz 3** **D-81829 München**	Lieferant der Software von Nuance – Dragon Anywhere
Newsletter2Go GmbH **Nürnberger Straße 8** **D-10787 Berlin**	Software für Newsletter System
Susell GmbH **Rosenthaler Straße 38** **D-10178 Berlin**	Software für digitale Kanzleiakademie www.huelskoetter.info/kanzleiakademie
weclapp SE **Neue Mainzer Straße 6668** **D-60311 Frankfurt am Main**	ERP-Software

42DBS GmbH **A Zejn Group Company** **c/o Mindspace Herzogspitalstraße 24** **D-80331 München**	Software für ShakeSpeare
TeamViewer Germany GmbH **Bahnhofsplatz 2** **D-73033 Göppingen**	Software für Fernwartung
METHODIGY GmbH **Richard-Hirschmann-Straße 5** **D-73728 Esslingen a.N.**	Software für METHODIGY
netgo Mannheim GmbH **Harrlachweg 5** **D-68163 Mannheim**	Hosting des Rechenzentrums für Juristen
AnyDesk Software GmbH **Friedrichstraße 9** **70174 Stuttgart**	Software für Fernwartung