Vertrag zur Auftragsdatenverarbeitung
nach Art. 28 ff. der EU – Datenschutz-Grundverordnung (DSGVO)

zwischen

Firma / Kanzlei ----------**als Auftraggeber**
Straße / Nr.
PLZ
Ort

vertreten durch
und
der

WOLLSCHLÄGER GBR **als Auftragnehmer**
vertreten durch die Gesellschafter Ariane und Hermann Wollschläger
Auf dem Sonnenberg 42
50389 Wesseling

Allgemeines
Als Auftragnehmer verarbeitet die WOLLSCHLÄGER GBR personenbezogene Daten ihrer Auftraggeber ausschließlich in deren Auftrag. Personenbezogene Daten werden nur erhoben, wenn Sie uns diese freiwillig mitteilen. Die WOLLSCHLÄGER GBR erhebt, verarbeitet und nutzt personenbezogene Daten, wie beispielsweise Name, Anschrift oder E-Mail-Adressen ohne weitergehende Einwilligung nur, soweit sie für die Vertragsbegründung und -abwicklung erforderlich sind. Grundlage dafür bildet der Wille unseres Auftraggebers zur Auftragsdatenverarbeitung i. S. d. Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO).

Wahrung berufsständischer Regeln
Als Unternehmen, das für Steuerberater, Wirtschaftsprüfer und Rechtsanwälte tätig ist, unterwirft sich die WOLLSCHLÄGER GBR, soweit das ihre Beratungs- und Serviceleistungen tangiert, den

- **Regeln der Berufssatzung der Wirtschaftsprüfer und Rechtsanwälte**
- **dem Steuerberatungsgesetz**
- **dem Berufsrecht der Wirtschaftsprüfer, Steuerberater und Rechtsanwälte**

Diese gesetzlichen Grundlagen, einschließlich der Vorschriften des BGB, regeln die Haftungs- und Sorgfaltspflichten im Geschäftsbetrieb. Alle Mitarbeiter sind **arbeitsvertraglich** in diese Vorschriften eingebunden.

Dauer des Auftrags
Die Vertragsdauer wird individuell im gesonderten Leistungsvertrag festgelegt und endet mit der Kündigung des Vertrages. Der Auftraggeber und der Auftragnehmer können den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt.

Gegenstand eines Auftrags kann sein
a) Beratung zu strategischen und organisatorischen Fragen
b) Erstellung und Pflege von Webseiten, Blogs, Einrichtung von Domains
c) Erstellung von Fachpublikationen
d) Bereitstellung von SaaS (Software as a Service), z. B. Kanzleitresor, Kasse, App, Newslettertool, E-Mail-Accounts, etc.

Zweck und Verwendung personenbezogener Daten bei Aufträgen von a) bis c)
Mit der Aufnahme des Auftrags speichert der Auftragnehmer persönliche Kontakt- und Adressdaten sowie Namen und Informationen, die ihm freiwillig in Gesprächen oder schriftlich vom Auftraggeber gegeben werden, nur soweit diese Informationen zur Erfüllung des Auftrags und zur Geltendmachung und Verteidigung von Rechten im Rahmen des Auftrags notwendig sind.
Die Rechtmäßigkeit und Notwendigkeit der Verarbeitung erfolgt nach Art. 6 DSGVO, um den Auftraggeber z. B. bei Webhostern, der DENIC etc. zu vertreten und Ansprüche von Behörden geltend machen zu können.

Art der Daten
Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien) Personenstammdaten Kommunikationsdaten (z. B. Telefon, E-Mail) Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse) Kundenhistorie Vertragsabrechnungs- und Zahlungsdaten Planungs- und Steuerungsdaten Auskunftsangaben (von Dritten, z. B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

Kategorien betroffener Personen
Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen: Kunden, Interessenten, Abonnenten, Beschäftigte, Lieferanten, Geschäftspartner, Subunternehmer, Ansprechpartner.
Die Daten werden vom Auftragnehmer auch bis zum Ablauf der gesetzlich festgelegten steuer- und handelsrechtlichen Aufbewahrungs- und Dokumentationspflichten gespeichert und danach gelöscht.

Weitergabe von Daten an Dritte
Eine Übermittlung von persönlichen Daten an Dritte (Behörden, Rechtsberatung, DENIC,Finanzverwaltung, Subunternehmer) findet nur statt, soweit sie für das Auftragsverhältnis erforderlich oder gesetzlich vorgeschrieben ist.

Zweck und Verwendung personenbezogener Daten bei Aufträgen – Bereitstellung von SaaS
Gegenstand des Auftrages ist die Bereitstellung von SaaS (Software as a Service) – Lösungen im Rahmen des mit dem Auftraggeber vereinbarten Umfangs, wie z. B. Kasse, Rechnungschreibung, elektronisches Kassenbuch, Kanzleitresor etc. SaaS-Anwendungen sind Entwicklungen unter der Regie unserer Subunternehmerin, der EDV-Beratung Dölle, Moerser Str. 103, 40667 Meerbusch, vertreten durch die Geschäftsführerin Gabriele Dölle https://www.edv-beratung-doelle.de. Die WOLLSCHLÄGER GBR übernimmt in der Zusammenarbeit den Vertrieb und Support. Die Subunternehmerin ist mit der WOLLSCHLÄGER GBR vertraglich nach den Regeln des DSGVO verbunden.
Die Daten in den SaaS-Anwendungen bringt der Auftraggeber selbst in die Systeme ein, verarbeitet, speichert und löscht unter seiner alleinigen Kontrolle Daten, die er selbst verschlüsselt.
Gegenstand des Auftrages ist deshalb **nicht** die originäre Nutzung oder Verarbeitung von personenbezogenen Daten durch den Auftragnehmer und seinen Subunternehmer. Im Zuge der Leistungserbringung des Auftragnehmers als Dienstleister im Bereich SaaS, des Supports bzw. der Administration von Server-Systemen kann ein Zugriff auf personenbezogene Daten jedoch nicht ausgeschlossen werden. Umfang, Art und Zweck der Zugriffsmöglichkeiten des Auftragnehmers auf Daten des Auftraggebers ergeben sich aus den einzelnen Produkten und Leistungsbeschreibungen.
Zusammenfassend entstehen die Zugriffsmöglichkeiten:

- beim Betreiben der Anwendungen (Backup, Restore, Web-Server)
- bei der technischen Administration der Server-Systeme
- bei sonstigen Support-Tätigkeiten für sämtliche Server-Systeme

Standorte der Datenverarbeitung
Alle Daten zu vertraglich vereinbarten Leistungen werden ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.
Alle Anwendungen befinden sich auf angemieteten Servern der großen zertifizierten europäischen Hoster von United-Internet, Hosteurope, Strato, Spectrum. Alle Anwendungen laufen grundsätzlich auf eigenen Servern. Die Hoster sind verantwortlich für die technische Infrastruktur, die Backbones mit mehrfach redundanten Anbindungen an mehrere Carrier und die beste Verfügbarkeit der Anwendungen.

Die Rechenzentren verfügen über einen Sicherheitsbereich mit einer Eingangskontrolle, sind in Geländen eingezäunt und mit Video überwacht. Neben der Überwachung finden regelmäßige Kontrollgänge durch das Sicherheitspersonal statt. Der Zutritt wird durch ein elektronisches Zutrittskontroll-System ermöglicht und somit wird der Zugang zum Data-Center nur autorisierten Personen ermöglicht.

Technisch-organisatorische Maßnahmen
Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus

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

Zugangskontrolle zu den Daten
Der Auftraggeber entscheidet alleine und ausschließlich darüber, welche personenbezogenen Daten in welcher Weise verarbeitet werden.
Alle Anwendungen werden durch einen individuellen Zugang kontrolliert. Beim Anlegen der Benutzer müssen bestimmte Kriterien für das Passwort und den Benutzernamen erfüllt sein, um einen neuen Benutzer erfolgreich aufsetzen zu können. Innerhalb der Anwendungen ist durch ein Rollen- und Rechte-System der Zugang nur zu den Daten möglich, die die jeweilige Rolle vorsieht.

Zugriffskontrolle
In allen Anwendungen wird der Zugriff auf die Daten mittels geeigneter Methoden kontrolliert. Vor fast jedem Datenbank-Zugriff wird kontrolliert, ob die selektierten Daten auch mit dem angemeldeten Benutzer eingesehen werden können. Auf Systemen mit besonders sensiblen Daten wird z. B. das sogenannte Session Hijacking dadurch verhindert, dass ein Benutzer nur ein einziges Mal zur gleichen Zeit angemeldet sein kann.

Eingabekontrolle
Innerhalb der Anwendungen ist für sensible Bereiche immer zu sehen, wer den Datensatz als Letzter verändert hat. Außerhalb der Anwendungen läuft eine sogenannte Log-Datei mit, die jeden Zugriff mit Datum, Uhrzeit und IP-Adresse protokolliert. Mit Hilfe dieser Dateien kann die aufgeführte Zielbeschreibung umgesetzt werden.

Weitergabekontrolle
Grundsätzlich erfolgt der Zugriff auf die Anwendungen über eine verschlüsselte Verbindung. So ist sichergestellt, dass während des Transports die Daten geschützt sind.
Alle administrativen Zugriffe auf die Server erfolgen über eine SSL-verschlüsselte Session.

Verfügbarkeitskontrolle
In den Rechenzentren der genutzten Hoster besteht i. d. R. mindestens eine unterbrechungsfreie Stromversorgung (USV) sowie ein Überspannungsschutz. Ebenso sind ein Branderkennungs- und Frühwarnsystem implementiert. Die Löschsysteme sind auf eine möglichst zerstörungsfreie Brandbekämpfung ausgelegt.
Zusätzlich werden die Sicherungen der einzelnen Server verschlüsselt auf jeweils einen weiteren Server abgelegt. So ist sichergestellt, dass bei einem Defekt eines Servers keine Daten verloren gehen.

Datentrennungskontrolle
Innerhalb der Anwendungen werden die Daten immer nur zu einem Zweck erhoben. Die einzelnen Anwendungen sind vollkommen voneinander getrennt (teilweise sogar in unterschiedlichen Rechenzentren).

Berichtigung, Einschränkung und Löschung von Daten
Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

Informationspflichten des Auftragnehmers
Der Auftragnehmer ist zur unverzüglichen Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen, verpflichtet. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

Kontrollrechte des Auftraggebers
Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers
Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.
Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.
Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

Der Auftraggeber ist berechtigt, vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.
Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

Unterauftragsverhältnisse
Der Auftragnehmer ist berechtigt, Unterauftragsverhältnisse einzugehen. Darunter sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z. B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

Löschung von Daten und Rückgabe von Datenträgern
Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial.

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

_____	_____**Wesseling 25.04.2018**
Ort, Datum	Ort, Datum
	
_____	_____
Auftraggeber	Auftragnehmer WOLLSCHLÄGER GBR Hermann Wollschläger Gesellschafter