Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO – Vereinbarung

Vereinbarung zwischen

Verantwortlicher - nachstehend Auftraggeber AG genannt

und

Grasenhiller GmbH, Sachsenstr. 2, 92318 Neumarkt

Geschäftsführer: Hermann Iberler

Auftragsverarbeiter - nachstehend Auftragnehmer AN genannt

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand: Der Gegenstand des Auftrags ergibt sich aus dem Dienstleistungsvertrag / Rahmenverträgen

☐ Dienstleistungsverträge für Kopier- & EDV-Systeme, Internet & E-Business, IT- & Softwarelösungen

☐ ALLIN-Vertrag / Servicevertrag Kopier- und Drucksysteme

☐ Hard- und Softwarebetreuungsvertrag – IT- & Softwarelösungen

☐ EDV-Servicevertrag – EDV-Systeme

☐ Defendo-Mietvertrag

☐ Internet-Service-Providing-Vertrag

Aufgrund dieser Verträge sind Zugriffe auf Daten möglich, die im Rahmen von Vertriebs, Verkaufs-, Support- oder Servicetätigkeiten anfallen und für eine ordnungsgemäße und optimale Ausführung aller Dienstleistungen zwingend notwendig sind.

(2) Dauer: Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von vier Wochen zum Monatsende gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Der Inhalt der Einzelaufträge ist in den Einzelverträgen detailliert erläutert; die Verarbeitung von Daten erfolgt im Rahmen der Abwicklung von Dienstleistungsaufträgen für

- Supporttätigkeiten
- Beratungs- und Betreuungsdienstleistungen

- Service-, Wartung und Reparatur von Hardware
- Erstellen und Verwalten von Verträgen

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des AG und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind. Das angemessene Schutzniveau wird hergestellt durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b i.V.m. Art. 47 DS-GVO);

(2) Art der Daten: Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten:

- Kundendaten (Kundennummer, Unternehmen, Ansprechpartner, Anschrift, Webseite, Kommunikationsdaten)
- Kontaktdaten (Name, Telefon, Fax, E-Mail)
- Abrechnungsdaten (Verbrauchswerte)
- Vertragsdaten (Kontaktdaten, Anschrift, vertragliche Interessen, Produkt, Leistungsbestandteile)
- Zahlungsdaten (Kontoinformation)
- Telekommunikationsdaten (Rufnummer, Verbindungsteilnehmer, Datum und Zeit der Verbindung
- Protokolldaten (Z. B. Logfiles über Nutzungsvorgänge)
- IP-Adressen

(3) Kategorien betroffener Personen: Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden
- Interessenten
- Lieferanten
- Kontaktpersonen
- Besucher
- Bewerber
- Beschäftigte
- Mitarbeiter externer Unternehmen

3. Technisch-organisatorische Maßnahmen

(1) Der AN hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem AG zur Prüfung zu übergeben. Bei Akzeptanz durch den AG werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des AG einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der AN hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO 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 DS-GVO zu berücksichtigen.
(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem AN gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der AN darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des AG berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den AN wendet, wird der AN dieses Ersuchen unverzüglich an den AG weiterleiten.
(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessen werden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des AG unmittelbar durch den AN sicherzustellen.

5. Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis Art. 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Der Auftragnehmer bestellt einen Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und Art. 39 DS-GVO ausübt, schriftlich.
   Als Datenschutzbeauftragter ist beim Auftragnehmer bestellt:

   Thomas M. Hofmann
   TMH-Dat UG (haftungsbeschränkt)
   Im Ostried 18
   87463 Dietmannsried
   Web: www.audaco.de

   Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

   Die Kontaktdaten des Datenschutzbeauftragten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Seine jeweils aktuellen Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der AN setzt 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. Der AN und jede dem AN unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des AG verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

d) Der AG und der AN arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) Die unverzügliche Information des AG über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim AN ermittelt.

f) Soweit der AG seinerseits 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 AN ausgesetzt ist, hat ihn der AN nach besten Kräften zu unterstützen.

g) Der AN kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem AG im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der AN 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 AG auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Die Auslagerung auf Subunternehmer oder der Wechsel des bestehenden Subunternehmers sind zulässig, soweit der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten schriftlich gegenüber dem Auftragnehmer Einspruch gegen die geplante Auslagerung erhebt.

(3) Mit dem Subunternehmer ist eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 3 und 4 DSGVO abzuschließen, die den Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit dieser Vereinbarung entspricht. Der Auftraggeber ist berechtigt, beim Auftragnehmer Einsicht in dessen Verträge mit Subunternehmern zu nehmen und vom Auftragnehmer die Übersendung einer Kopie dieser Verträge zu verlangen.

(4) Die bestehenden Unterauftragsverhältnisse des Auftragnehmers sind in Anlage 1 zu diesem Vertrag angeben.

7. Kontrollrechte des Auftraggebers

(1) Der AG hat das Recht, im Benehmen mit dem AN 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 AN in dessen Geschäftsbetrieb zu überzeugen.

(2) Der AN stellt sicher, dass sich der AG von der Einhaltung der Pflichten des AN nach Art. 28 DS-GVO überzeugen kann. Der AN verpflichtet sich, dem AG auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann wahlweise erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Für die Ermöglichung von Kontrollen durch den AG kann der AN einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der AN unterstützt den AG bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, 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 personenbezogener Daten unverzüglich an den AG zu melden
c) die Verpflichtung, dem AG im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
d) die Unterstützung des AG für dessen Datenschutz-Folgenabschätzung

e) die Unterstützung des AG im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des AN zurückzuführen sind, kann der AN eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Falls vom Auftragnehmer keine näheren Angaben zu den weisungsempfangsberechtigten Personen gemacht werden, kann der Auftraggeber davon ausgehen, dass alle Mitarbeiter des Auftragnehmers weisungsempfangsberechtigt sind.

(2) Mündliche Weisungen bestätigt der AG unverzüglich (mind. Textform).

(3) Der AN hat den AG unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der AN ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den AG bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des AG nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den AG – spätestens mit Beendigung der Leistungsvereinbarung – hat der AN sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem AG auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

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

11 . Haftung

Auf Art. 82 DS - GVO wird verwiesen.

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Unterschrift AG	Unterschrift AN

Anlage 1

Unterauftragnehmer

Der Auftragnehmer kann für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch nehmen, die in seinem Auftrag Daten verarbeiten.

Dabei handelt es sich um nachfolgende Unternehmen:

- Hetzner Online GmbH, Gunzenhausen
- Acmeo GmbH, Mailänder Straße 2 / Expo Plaza, 30539 Hannover