# Vereinbarung über eine Auftragsverarbeitung gemäß Art. 28 DSGVO

**Der Verantwortliche: (im Folgenden Auftraggeber)**

**Der Auftragsverarbeiter: (im Folgenden Auftragnehmer)**
Esther Kobula, Mosern 19, 9421 Eitweg

## 1. Gegenstand der Vereinbarung

### 1) Gegenstand

☐ Der Gegenstand dieses Auftrages ist die Durchführung folgender Aufgaben durch den Auftragnehmer: Grafik- & Webdesign, Druckabwicklung.

☐ Der Gegenstand des Auftrags ergibt sich aus einem Rahmenvertrag, Werkvertrag, Leistungsvereinbarung, vom , auf die hier verwiesen wird. Diese Vereinbarung ist als Ergänzung zu [1] zu verstehen.

### 2) Art und Zweck der Verarbeitung von Daten

☐ Nähere Beschreibung des Auftrages in Hinblick auf Art und Zweck der vorgesehenen Verarbeitung durch den Auftragnehmer.

☐ Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung vom jeweiligen Auftrag.

### 3) Art der Daten

Folgende Datenkategorien werden verarbeitet: Kontaktdaten, Kundendaten, Firmendaten, Zugangsdaten, Druckdaten.

### 4) Kategorien betroffener Personen

Folgende Kategorien betroffener Personen unterliegen der Verarbeitung: Auftraggeber.

## 2. Dauer der Vereinbarung

☐ Einmalige Durchführung Der Auftrag wird zur einmaligen Durchführung erteilt; die Vereinbarung endet nach Ausführung der Arbeiten.

☐ Befristete Laufzeit Die Vereinbarung ist befristet abgeschlossen und endet mit [2].

☐ Unbefristete Laufzeit Die Vereinbarung ist auf unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von einem Monat zum Quartal gekündigt werden. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

## 3. Pflichten des Auftragnehmers

**1)** Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Kopien oder Duplikate der Daten werden ohne Wissen des Auf-

traggebers 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)** Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragnehmers eines schriftlichen Auftrages.

**3)** Wahrung der Vertraulichkeit und Verschwiegenheit: Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

**4)** Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32ff DSGVO ergriffen hat. Konkret handelt es sich hierbei um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Einzelheiten hierzu finden sich im Anhang (Technisch-organisatorische Maßnahmen).

**5)** Mitwirkungspflicht bei Betroffenenrechten: Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Betroffenenrechte nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen. Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.

**6)** Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer durchzuführen (sicherzustellen).

**7)** Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten. Dazu gehören Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation.

**8)** Der Auftragnehmer wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu erstellen hat.

**9)** Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch ihn beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

**10)** Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, sämtliche in seinem Besitz gelangten Unterlagen, erstellte Verarbeitungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber zu übergeben / in dessen Auftrag zu vernichten3. Wenn der Auftragnehmer die Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder nach Wunsch des Auftraggebers in dem Format, in dem er die Daten vom Auftraggeber erhalten hat oder in einem anderen, gängigen Format herauszugeben. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

**11)** Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

## 4. Technisch-organisatorische Maßnahmen

Die technischen und organisatorischen Maßnahmen (TOMs) unterliegen dem technischen Fortschritt und der Weiterentwicklung. Es ist dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen, soweit das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren. Einzelheiten sind dem Anhang zu entnehmen.

## 5. Ort der Durchführung der Datenverarbeitung

☐ Ausschließliche Durchführung innerhalb der EU/des EWR Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw des EWR durchgeführt.

☐ Bei Durchführung, wenn auch nur teilweise, außerhalb der EU/des EWR Datenverarbeitungstätigkeiten werden zumindest zum Teil auch außerhalb der EU bzw des EWR durchgeführt, und zwar in [4].
Das angemessene Datenschutzniveau ergibt sich aus[5]

- ☐ einem Angemessenheitsbeschluss der Europäischen Kommission nach Art 45 DSGVO.
- ☐ einer Ausnahme für den bestimmten Fall nach Art 49 Abs 1 DSGVO. verbindlichen internen Datenschutzvorschriften nach Art 47 iVm Art 46 Abs 2 lit b DSGVO.
- ☐ Standarddatenschutzklauseln nach Art 46 Abs 2 lit c und d DSGVO.
- ☐ genehmigten Verhaltensregeln nach Art 46 Abs 2 lit e iVm Art 40 DSGVO.
- ☐ einen genehmigten Zertifizierungsmechanismus nach Art 46 Abs 2 lit f iVm Art 42 DSGVO.
- ☐ von der Datenschutzbehörde bewilligte Vertragsklauseln nach Art 46 Abs 3 lit a DSGVO.
- ☐ einer Ausnahme für den Einzelfall nach Art 49 Abs 1 Unterabsatz 2 DSGVO.

## 6. Sub-Auftragsverarbeiter

☐ Verbot der Hinzuziehung eines Sub-Auftragsverarbeiters Der Auftragnehmer ist nicht berechtigt, einen Sub-Auftragsverarbeiter zur unmittelbaren Erbringung der Hauptdienstleistung heranzuziehen.

☐ Zulässigkeit der Hinzuziehung eines bestimmten Sub-Auftragsverarbeiters Der Auftragnehmer ist befugt folgendes Unternehmen als Sub-Auftragsverarbeiter zur unmittelbaren Erbringung der Hauptdienstleistung hinzuziehen: [6].

☐ Zulässigkeit der Hinzuziehung von Sub-Auftragsverarbeitern Der Auftragnehmer kann Sub-Auftragsverarbeiter, z.B. Druckereien, hinzuziehen. Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer dies dem Auftraggeber eine angemessene Zeit vorab schriftlich anzeigt und
- der Auftraggeber nicht gegenüber dem Auftragnehmer schriftlich Einspruch gegen die geplante Auslagerung erhebt und
- die erforderlichen Vereinbarungen zwischen dem Auftragnehmer und dem Sub-Auftragsverarbeiter gemäß des Art. 28 Abs. 4 DSGVO abgeschlossen werden. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragnehmer auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

Ort, Datum (Auftraggeber)

Ort, Datum (Auftragnehmer)

# Anhang – Technisch-organisatorische Maßnahmen (TOMs)[7]

**Allgemeine Beschreibung der technisch-organisatorischen Maßnahmen**

**a. Vertraulichkeit8:**
**Büro:** Zutrittskontrolle (Wird nach Verlassen versperrt)
**PC:** Zugriffskontrolle durch Passwortabfrage, Verschlüsselung von E-Mail Verkehr, Das Firmen WLAN ist verschlüsselt, Bei zukünftigen Updates/Neukauf von Software wird auf die Einhaltung der DSGVO großen Wert gelegt.
**Mobil:** Zugriffskontrolle durch Biometrie

**b. Integrität[9]:**
Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung: SSL Verschlüsselung der E-Mails Andere Portale wie z. B. (Dropbox, Google Drive) werden nicht verwendet

**c. Verfügbarkeit und Belastbarkeit:** Backup, Ausfallsicherheit durch Raid 5, Virenscanner (G-Data) Firewall im Zulauf.

**d. Pseudonymisierung und Verschlüsselung:**
Momentan nicht implementiert. Bei zukünftigen Updates/Neukauf von Software wird auf die Einhaltung der DSGVO großen Wert gelegt.

**e. Evaluierungsmaßnahmen:**
Datenträger werden vor ihrer Entsorgung überschrieben und physisch zerstört, sodass die darauf enthaltenen Daten nicht wiederhergestellt werden können.