Vertrag über Auftragsdatenverarbeitung

gemäß Art. 28 DSGVO

zwischen

_____

_____

_____

vertreten durch

_____

- Auftraggeber -

und

Westenberg + Küppers GbR
Spanische Schanzen 37
47495 Rheinberg

vertreten durch
Patrick Westenberg / Sebastian Küppers

- Auftragnehmerin -

schließen zur Kundennummer

10_____

nachfolgenden Vertrag über die Verarbeitung personenbezogener Daten

1. **Allgemeines**
   (1) Die Auftragnehmerin verarbeitet personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage dieses Vertrages.
   (2) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung (von Daten)“ benutzt wird, wird damit allgemein die Verwendung von personenbezogenen Daten verstanden. Eine Verwendung personenbezogener Daten umfasst insbesondere die Erhebung, Speicherung, Übermitlug, Sperrung, Löschung, Anonymisierung, Pseudonymisierung, Verschlüsselung oder sonstige Nutzung von Daten.

2. **Gegenstand des Auftrags**
   (1) Der Auftrag des Auftraggebers an die Auftragnehmerin umfasst Leistungen der Bereiche (bitte zutreffendes ankreuzen):
   [ ] Webhosting
   [ ] Domainregistrierung und -verwaltung
   [ ] vServer
   [ ] E-Mail-Verarbeitung
   [ ] Serverhousing
   [ ] _____
   im Rahmen der von der Auftragnehmerin angebotenen und in den jeweiligen Leistungsbeschreibungen und Verträgen konkretisierten Produkte.
   (2) Die vertraglich vereinbarten Dienstleistungen werden in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Es sei denn, eine Übermittlung zwingend notwendiger Daten an Registrierungsstellen in Drittländer ist zur Erfüllung eines Vertrages mit der betroffenen Person oder zum Abschluss oder zur Erfüllung eines Vertrages im Interesse der betroffenen Person erforderlich. Diese Übermittlung ist aufgrund Art. 49 Abs. 1 Satz 1, lit. b und c DSGVO zulässig. Welche Daten zwingend übermittelt werden ist abhängig von der zuständigen Registrierungsstelle in dem jeweiligen Drittland, um eine Domainregistrierung schnellstmöglich durchführen zu können.
   (3) Folgende Datenarten sind Gegenstand der Verarbeitung (bitte zutreffendes ankreuzen):
   [ ] Adressdaten
   [ ] Abrechnungsdaten
   [ ] Bankverbindungsdaten
   [ ] Bestelldaten
   [ ] E-Mail-Nachrichten
   [ ] Mitarbeiterdaten
   [ ] Vertragsdaten
   [ ] Stammdaten
   [ ] Nutzungsdaten
   [ ] _____
   (4) Kreis der von der Datenverarbeitung Betroffenen (bitte zutreffendes ankreuzen):
   [ ] Kunden
   [ ] Nutzer
   [ ] Lieferanten
   [ ] Mitarbeiter
   [ ] Bewerber
   [ ] Interessenten
   [ ] Geschäftspartner
   [ ] Mitglieder
   [ ] Dienstleister
   [ ] Praktikanten

3. **Rechte und Pflichten des Auftraggebers**
   (1) 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.
   (2) Der Auftraggeber ist berechtigt sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der bei der Auftragnehmerin getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen. Der Auftraggeber ist verpflichtet, das Ergebnis in geeigneter Weise zu dokumentieren.
   (3) Der Auftraggeber hat das Recht, Weisungen über Art, Umfang und Verfahren der Datenverarbeitung schriftlich zu erteilen. Es obliegt dem Auftraggeber, Daten vor Beendigung des Vertrages umzuziehen beziehungsweise eine Sicherungskopie anzufertigen. Der Auftraggeber hat selbst Zugriff auf seine Daten, insofern trifft die Auftragnehmerin keine Pflicht zur Herausgabe. Die Obliegenheit des Auftraggebers zur Datensicherung während der Vertragslaufzeit bleibt hiervon unberührt.
   (4) Der Auftraggeber erteilt alle Aufträge oder Teilaufträge und Weisungen schriftlich oder in einem dokumentierten elektronischen Format. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und unverzüglich schriftlich oder in einem dokumentierten elektronischen Format festzulegen.
   (5) Der Auftraggeber kann weisungsberechtigte Personen schriftlich benennen. Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies der Auftragnehmerin unverzüglich schriftlich mitteilen.
   (6) Der Auftraggeber informiert die Auftragnehmerin unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
   (7) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der Auftragnehmerin vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.
   (8) Dem Auftraggeber obliegen die aus Art. 33, 34 DSGVO resultierenden Informationspflichten. Im Rahmen der Übermittlung an Drittländer hat der Auftraggeber die betroffene Person in verständlicher Form über den konkreten Zweck der Datenübermittlung, die genauen Kategorien der zu übermittelnden Daten, der Kategorien der Empfänger, das Fehlen eines angemessenen Datenschutzniveaus (Aufklärung über fehlenden Angemessenheitsbeschluss, Fehlen geeigneter Garanten) und mögliche Risiken zu informieren.

4. **Pflichten der Auftragnehmerin**
   (1) Die Auftragnehmerin verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der

Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO). Soweit einzelne Weisungen den vertraglich vereinbarten Leistungsumfang übersteigen, sind die dadurch begründeten Kosten vom Auftraggeber zu tragen.

(2) Die Auftragnehmerin verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.

(3) Die Auftragnehmerin sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu.

(4) Die Auftragnehmerin verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort. Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf die Auftragnehmerin nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

(5) Die Auftragnehmerin wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Die Auftragnehmerin ist berechtigt, die Durchführung der betreffenden Weisung(en) solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

(6) Die Auftragnehmerin teilt dem Auftraggeber unverzüglich Störungen, Verstöße der Auftragnehmerin oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO. Die Auftragnehmerin sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf die Auftragnehmerin nur nach vorheriger Weisung durchführen.

(7) Die Auftragnehmerin kann dem Auftraggeber Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind.

(8) Die Auftragnehmerin sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden

Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO).

5. **Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit.d DSGVO)**
   (1) Der Auftraggeber stimmt zu, dass die Auftragnehmerin zur Erfüllung der vertraglich vereinbarten Leistungspflichten verbundene Unternehmen der Auftragnehmerin heranziehen oder dritte Unternehmen mit Leistungen unterbeauftragen kann. Hierzu erklärt sich der Auftraggeber ausdrücklich einverstanden (Art. 28 Abs. 2 DSGVO).
   (2) Die Auftragnehmerin sichert zu den Auftraggeber über die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers umfassend zu informieren. Die Auftragnehmerin trägt dafür Sorge, dass dass sie den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt.
   (3) Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO).
   (4) Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DSGVO bezüglich seiner Beschäftigten erfüllt hat.
   (5) Erteilt die Auftragnehmerin Aufträge an Subunternehmer, so obliegt es der Aufragnehmerin, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.
   (6) Die Auftragnehmerin informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (Art. 28 Abs. 2 Satz 2 DSGVO).
   (7) Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 f. DSGVO erfüllt sind.

6. **Kontrollbefugnisse**
   (1) Die Auftragnehmerin erklärt sich damit einverstanden, dass der Auftraggeber – grundsätzlich nach Terminvereinbarung – berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DSGVO).
   (2) Die Auftragnehmerin sichert zu, dass sie, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

(3) Etwaige durch die Wahrnehmung von Kontrollrechten der Auftragnehmerin entstehende Aufwendungen sind durch den Auftraggeber zu erstatten.

7. **Wahrung von Betroffenenrechten**
   (1) Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat die Auftragnehmerin im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. e und f DSGVO).
   (2) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers bei der Auftragnehmerin entstehen, bleiben unberührt.

8. **Löschung und Rückgabe von Daten, Beendigung des Auftrags (Art. 28 Abs. 3 Satz 2. lit. g DSGVO)**
   (1) Überlassene Datenträger und Datensätze verbleiben im Eigentum des Auftraggebers.
   (2) Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung durch den Auftraggeber jedoch spätestens mit Beendigung der Leistungsvereinbarung hat die Auftragnehmerin sämtliche in ihren Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigte Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung des Auftraggebers datenschutzgerecht zu vernichten (Art. 17 Abs. 1 DSGVO). Gleiches gilt für Test- und Ausschussmaterial.
   (3) Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.
   (4) Die Auftragnehmerin kann Dokumentationen, die dem Nachweis der Auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahren. Alternativ kann sie diese zu ihrer Entlastung bei Vertragsende dem Auftraggeber übergeben.

9. **Technische und organisatorische Maßnahmen**
   siehe Anlage „Technische und organisatorische Maßnahmen“

10. **Geheimhaltungspflichten**
    (1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben

genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

11. **Vertragslaufzeit**

(1) Die Laufzeit dieser Vereinbarung entspricht der Laufzeit des Hauptvertrages und Kundenverhältnisses. Sollten Leistungen auch noch nach Beendigung des Hauptvertrages erbracht werden, gelten die Regelungen dieser Vereinbarung auch für diese weitere Leistungserbringung für die gesamte Dauer der tatsächlichen Kooperation fort.

12. **Schlussbestimmungen**

(1) Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

(2) Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

(3) Sollte das Eigentum des Auftraggebers bei der Auftragnehmerin durch Maßnahmen Dritter(etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat die Auftragnehmerin den Auftraggeber unverzüglich zu informieren. Die Auftragnehmerin wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

(4) Die Einrede des Zurückbehaltungsrechts i.S.v. §273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(5) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

(6) Änderungen und Ergänzungen am Vertragstext außerhalb der zu Ziffer 2 möglichen ergänzenden Angaben sind unwirksam.

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Unterschrift - Auftraggeber -	Unterschrift - Auftragnehmerin -

Anlage zum Vertrag über Auftragsdatenverarbeitung nach DSGVO

Technische und organisatorische Maßnahmen (TOM)

1. Zutrittskontrolle

- Büros der Auftragnehmerin
  - ✔ beschränkter Zugang (Türschließung, Begleitung durch Mitarbeiter der AN)
- Rechenzentrum
  - ✔ Zutritt nur nach vorheriger Anmeldung
  - ✔ Personenkontrolle beim Eingang
  - ✔ Elektronisches Zutrittskontrollsystem (Chipkarten-Schließsystem) mit Protokollierung
  - ✔ Dokumentierte Chipkartenvergabe an Zutrittsberechtigte
  - ✔ 24/7 personelle Besetzung der Rechenzentren
  - ✔ Videoüberwachung von Serverräumen und Korridoren
  - ✔ Rechenzentren sind alarmgesichert
  - ✔ Rechenzentren sind nicht als solche gekennzeichnet

2. Zugangskontrolle

- Verwaltungssysteme der Auftragnehmerin
  - ✔ Benutzername und Passwort
  - ✔ 2-Faktor-Authentifizierung
  - ✔ Einsatz einer Software-Firewall
  - ✔ Einsatz von VPN-Technologie

- Serverhousing
  - ✔ Die Verantwortung der Zugangskontrolle obliegt ausschließlich dem Auftraggeber

3. Zugriffskontrolle

- Serverhousing
  - ✔ Die Verantwortung der Zugriffskontrolle obliegt ausschließlich dem Auftraggeber

4. Weitergabekontrolle

- Anwendung gängiger Transportverschlüsselung (SSL-, TLS-, STARTTLS-Verbindungen)
- Verwendung gängiger VPN-Technologien

5. Eingabekontrolle

- Verwaltungssysteme der Auftragnehmerin
  - ✔ Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
  - ✔ Die Verantwortung der Eingabekontrolle obliegt dem Auftraggeber

6. Auftragskontrolle

- Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung imAuftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers. Die Datenschutzerklärung enthält detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers.

- Die Datenschutzerklärung enthält detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers.

7. Verfügbarkeitskontrolle

- Verwaltungssysteme der Auftragnehmerin
  - ✔ tägliche Sicherung aller relevanten Daten, verschlüsselte Übertragung
  - ✔ Einsatz von Schutzprogrammen (Virenscanner, Spamfilter)
  - ✔ Einsatz einer Software-Firewall
  - ✔ Einsatz von VPN-Technologie
  - ✔ unterbrechungsfreie Stromversorgung (USV)
  - ✔ Klimaanlage in Serverräumen
  - ✔ Feuer- und Rauchmeldeanlagen
  - ✔ Feuerlöschgeräte in Serverräumen

- Serverhousing
  - ✔ Datensicherung obliegt dem Auftraggeber
  - ✔ unterbrechungsfreie Stromversorgung (USV)
  - ✔ Klimaanlage in Serverräumen
  - ✔ Feuer- und Rauchmeldeanlagen
  - ✔ Feuerlöschgeräte in Serverräumen

8. Trennungskontrolle zur Datensicherung (physikalisch / logisch)

- Verwaltungssysteme der Auftragnehmerin
  - ✔ Daten werden physikalisch oder logisch von anderen Daten getrennt
  - ✔ Die Datensicherung erfolgt auf logisch und/oder physikalisch getrennte Systeme

- Serverhousing
  - ✔ Die Trennungskontrolle obliegt dem Auftraggeber