Vertrag zur Auftragsverarbeitung i.S.d. Art. 28 Datenschutz-Grundverordnung (DS-GVO)

Der Verantwortliche:

Firmenwortlaut: ……

Anschrift: ……

PLZ, Ort: ……

Land: ……

Verantwortlicher: ……

(im Folgenden: Auftraggeber)

Der Auftragsverarbeiter:

Firmenwortlaut:	Westnet GmbH
Anschrift:	Telepark 1
PLZ, Ort:	A – 8572 Bärnbach

(im Folgenden: Auftragnehmer)

PRÄAMBEL

Westnet GmbH erbringt für seine Kunden verschiedene Leistungen im Bereich IT-Infrastruktur. Kerntätigkeit ist die Zurverfügungstellung von Serverinfrastruktur und Dienstleistungen (Services) an seine Kunden. Dazu werden Leistungen in folgenden Bereichen erbracht:

- Domain Registrierung
- Webhosting (Webserver, FTP-Server, Datenbank-Server)
- eMail-Services (Transport und Zustellung von eMails, Antivirus, Spamfilterung)
- Serverhousing (Kunden-Server od. Speichersysteme)
- Zurverfügungstellung von virtuellen Server-Ressourcen

Um o.g. Leistungen für seine Kunden erbringen zu können, werden personenbezogene Daten (gem. Art. 4 Z1 DSGVO) dieser, verarbeitet.

Die Verarbeitung (gem. Art. 4 Z2 DSGVO) ist für die Erfüllung der vertraglichen Vereinbarung zwischen Auftraggeber und Auftragnehmer (Westnet) notwendig.

GEGENSTAND DER VEREINBARUNG

Diese Vereinbarung ist als Ergänzung zum Leistungsvertrag mit dem Auftragnehmer (Westnet) zu verstehen. Ein Vertrag zwischen dem Auftragnehmer (Westnet) und dem Auftraggeber kommt rechtlich zu Stande, wenn der Auftraggeber einen schriftlichen Vertrag mit dem Auftragnehmer (Westnet) abschließt. Der Auftraggeber erhält neben dem Vertrag zur Leistungsvereinbarung auch diese Vereinbarung über eine Auftragsverarbeitung nach Art. 28 DSGVO.

(1) Gegenstand dieses Auftrages ist die Durchführung folgender vertraglich vereinbarten Leistungen:

- Zurverfügungstellung einer Serverinfrastruktur und ggf. Services
- der Auftragnehmer verarbeitet zum Zweck der vorstehenden Leistungserbringung die Daten des Auftraggebers („Kundendaten“), um seine Leistungen abrechnen zu können bzw. die vom Kunden bestellten Leistungen erbringen zu können (z.B. eine Domainregistrierung vornehmen zu können)
- für sämtliche anderweitigen Daten des Auftraggebers (Uploads von Daten auf die bereitgestellte Infrastruktur und die Nutzung der Services durch den Auftraggeber) ist dieser selbst verantwortlich. Der Auftragnehmer (Westnet) stellt lediglich die Infrastruktur zur Verfügung
- Zurverfügungstellung von Räumlichkeiten (Rack, Regal, etc.) für Kundengeräte

(2) Folgende Datenkategorien werden verarbeitet:

- Geschlecht, Firmenname / Familienname, Vorname (bei natürlichen Personen), Titel, Adresse, Telefonnummer, E-Mail-Adresse (werden gem. DSGVO als personenbezogene Daten behandelt)
- Kontodaten (IBAN), Abbuchungsaufträge (werden gem. DSGVO als sensible Daten behandelt)
- Zugangsdaten (Benutzerdaten)

(3) Folgende Kategorien betroffener Personen unterliegen der Verarbeitung:

- Kunden, Ansprechpartner

2. DAUER DER VEREINBARUNG

Die Vereinbarung wird auf unbestimmte Zeit abgeschlossen und ist unmittelbar mit dem Kauf der Leistungen begründet. Die Dauer dieser Vereinbarung ist mit der Dauer der Nutzung der Leistungen des Auftragnehmers (Westnet) gekoppelt.

Der Auftraggeber stimmt ausdrücklich überein, dass sich die Dauer dieser Vereinbarung auf die Dauer des bestehenden Leistungsvertrages bezieht und bei ausgelaufenen oder gekündigten Verträgen noch auf die vereinbarte Speicherdauer des Auftragnehmers (Westnet) erstreckt (vgl. dazu Anhang – Abschnitt „Löschungsfristen“.

PFLICHTEN DES AUFTRAGNEHMERS

(1) Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der vereinbarten Leistungen des Auftraggebers zu verarbeiten. Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er – sofern gesetzlich zulässig bzw. falls keine andere Weisung von Behördenseite vorliegt (z.B. richterliche Verfügung, Befehl, Verordnung, u.ä)– den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen.

(2) 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.

(3) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art. 32 DSGVO ergriffen hat (Einzelheiten sind der Anlage zu entnehmen).

(4) Der Auftragnehmer ergreift hinreichende technische und organisatorische Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Person 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. 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.

(5) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten (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).

(6) Der Auftragnehmer erklärt, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art. 30 DSGVO errichtet hat.

(7) Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Prüfung der Datenverarbeitungseinrichtungen eingeräumt. Diese Prüfung kann durch ihn oder auch durch ihn beauftragte Dritte erfolgen. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen in Schriftform zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind. Die Parteien kommen ausdrücklich überein, dass dieser Kontrollmöglichkeit seitens des Auftragnehmers (Westnet) in der Anlage dieser Vereinbarung vollständig entsprochen wird.

(8) Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten in dessen Auftrag zu löschen. Ausgenommen von der Löschung und/oder Vernichtung sind jene Daten, für die es anderweitige gesetzliche Aufbewahrungspflichten gibt. 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.

(9) 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.

ORT DER DURCHFÜHRUNG DER DATENVERARBEITUNG

Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU durchgeführt.

SUB-AUFTRAGSVERARBEITER

Der Auftragnehmer ist nicht berechtigt, einen Sub-Auftragsverarbeiter heranzuziehen.

Beabsichtigte Änderungen hinsichtlich der Beschäftigung von Sub-Auftragsverarbeitern sind dem Auftraggeber rechtzeitig schriftlich bekannt zu geben, dass er diesen allenfalls widersprechen oder diese untersagen kann.

Bei einer Genehmigung durch den Auftraggeber ist der Auftragnehmer verpflichtet, die erforderlichen Vereinbarungen im Sinne des Art. 28 Abs. 4 DSGVO mit jeden einzelnen Sub-Auftragsverarbeiter abzuschließen. 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:	Bärnbach, am 18.05.2018
Für den Auftraggeber:	Für den Auftragnehmer:
……..……	……..
Name:	Günter Rathswohl, MBA
Funktion	Geschäftsführer

ANLAGE – TECHNISCH-ORGANISATORISCHE MASSNAHMEN

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung, insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen, sofern dabei das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten wird. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen.

VERTRAULICHKEIT

- Zutrittskontrolle: Physischer Zugriff auf die Infrastruktur des Auftragnehmers (Westnet) erfolgt ausschließlich durch befugte Personen mittels Schlüssel bzw. Transponder Schließsystem (Zutritt zu den Räumlichkeiten). Zusätzlicher Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen gewährleisten Sicherheitspersonal und Alarmanlagen rund um die Uhr;

- Zugangskontrolle: Schutz vor unbefugter Systembenutzung bzw. Zugriff auf die Infrastruktur des Auftragnehmers (Westnet) erfolgt ausschließlich durch befugte Personen. Dabei kommen Sicherheitsprotokolle auf dem jeweiligen aktuellsten Stand der Technik sowie digitale Signaturen zum Einsatz.

- Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Standard-Berechtigungsprofile auf „need to know-Basis“, Standardprozess für Berechtigungsvergabe, Protokollierung von Zugriffen, periodische Überprüfung der vergebenen Berechtigungen, insb. von administrativen Benutzerkonten

- Pseudonymisierung: die als sensibel eingestuften Daten (z.B. IBAN) werden in der jeweiligen Datenanwendung gesondert, verschlüsselt und pseudonymisiert aufbewahrt.

INTEGRITÄT

- Weitergabekontrolle: der Auftragnehmer stellt die Infrastruktur zur Verfügung: es findet zu keinem Zeitpunkt ein Zugriff auf die Daten der Kunden auf der für den Auftraggeber bereitgestellten Infrastruktur statt.

- Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung

VERFÜGBARKEIT UND BELASTBARKEIT

- Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV, Dieselaggregat), Virenschutz, Firewall, Meldewege und Notfallpläne; Security Checks auf Infrastruktur- und Applikationsebene, mehrstufiges Sicherungskonzept, Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern;

- Wiederherstellbarkeit und Backup Policies: um eine optimale Verfügbarkeit der Leistung für seine Kunden zu ermöglichen, nimmt der Auftragnehmer folgende Sicherungs- bzw. Backup Prozedere vor:

  - Laufende Verträge: im Bereich Webhosting und eMail-Services: Backups der letzten 30 Tage (ältere Daten als 30 Tage werden per Grundeinstellung gelöscht und sind nicht wiederherstellbar gem. Art. 25 Abs. 1 – Privacy by Design)

  - Ausgelaufene oder gekündigte Verträge: Daten von Webseiten und Inhalte von eMail-Konten werden noch 3 Monate auf Backups gespeichert. Nach dieser Frist werden Daten per Grundeinstellung gelöscht und sind nicht wiederherstellbar gem. Art. 25 Abs. 1 – Privacy by Design)

  Protokolle auf Webservern werden 30 Tage aufbewahrt. Logdateien werden im Rahmen von Debugging und zur Fehlersuche herangezogen. Diese fallweise Verarbeitung erfolgt ausschließlich durch Mitarbeiter des Auftragnehmers. Logdateien sind getrennt von anderen Datenbanken und werden auch mit keinen Datenbanken zusammengeführt (“big data”).

  Protokolle auf Mailservern (“Logdateien”) werden 30 Tage aufbewahrt. Diese Logdateien werden mit keinen anderen Datenbanken verknüpft (“big data”) und dienen dazu, den Transport von eMails nachvollziehen zu können und damit verbundene Fehler auf dem Transportweg aufzeigen zu können.

  Diese fallweise Verarbeitung erfolgt ausschließlich durch Mitarbeiter des Auftragnehmers. Der Auftraggeber hat keinen Zugriff auf Logdateien, weshalb seitens des Auftraggebers keine Behandlung im Sinne der DSGVO erforderlich ist.

- Löschungsfristen: wie im vorangegangenen Punkt dargestellt. Die Löschung erfolgt für Backups und Logdateien per Grundeinstellung gem. Art. 25 – Privacy by Design, Privacy by Default.

  - Virtuelle Server werden nach einer Kündigung durch den Kunden (sofortige Wirkung oder per Stichtag) bzw. nach der ersten unbezahlten Rechnung unmittelbar „Suspendiert“ und nach weiteren 7 Kalendertagen automatisch gelöscht.

  - Kunden-Server od. sonstige Speichereinheiten müssen nach einer Kündigung durch den Kunden (sofortige Wirkung oder per Stichtag) bzw. nach der ersten unbezahlten Rechnung innerhalb eines (1) Monats nach der Kündigung vom Auftraggeber aus den Serverräumlichkeiten unter Aufsicht des Auftragnehmers entfernt werden.

VERFAHREN ZUR REGELMÄSSIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

- Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen;
- Bereits Durchgeführte und regelmäßige Überprüfung der Datenschutzfolgeabschätzung
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen;