Vereinbarung zur Auftragsverarbeitung

zwischen

Kunde

– nachstehend *„Kunde“ oder „Auftraggeber“* genannt –

und

htp GmbH, Mailänder Str. 2, 30539 Hannover

– nachfolgend „htp“ oder „Auftragnehmer“ genannt -
– beide zusammen „Parteien“ genannt –

Der Kunde hat mit der htp einen Vertrag über folgendes Produkt geschlossen:

htp Net Business Hosting

(Webhosting, Webalizer, Domain, E-Mail)

Der Kunde nutzt das Produkt geschäftsmäßig.

Gegenstand dieser Vereinbarung ist die Regelung der Rechte und Pflichten des Verantwortlichen (Kunde oder Auftraggeber) und des Auftragnehmers (htp), sofern im Rahmen der Leistungserbringung eine Verarbeitung personenbezogener Daten durch die htp im Auftrag des Kunden im Sinne des Datenschutzrechts erfolgt.

Sie besteht aus diesem Vertragsdokument und den folgenden weiteren Dokumenten:

- Anlage 1 – Ergänzende Bedingungen der Auftragsverarbeitung
- Anlage 2 – Beschreibung der Datenverarbeitungstätigkeiten
- Anlage 3 – Technische und organisatorische Maßnahmen

Diese Vereinbarung ersetzt die bislang bestehenden vertraglichen Regelungen zum Datenschutz. Im Übrigen bleiben die bestehenden vertraglichen Regelungen unverändert.

htp GmbH	Kunde:
_____	_____
Ort, Datum	Ort, Datum
_____	_____
Rechtsverbindliche Unterschrift htp	Rechtsverbindliche Unterschrift Kunde
_____	_____
Name in Druckschrift	Name in Druckschrift

Anlage 1 – Ergänzende Bedingungen Auftragsverarbeitung

1. Gegenstand und Dauer des Auftrags

1.1 Gegenstand des Auftrags

Der Gegenstand des Auftrags sowie Art und Zweck der Verarbeitung ergeben sich aus dem Hauptvertrag und den mitgeltenden Dokumenten (insbes. AGB, Leistungsbeschreibungen) und sind in der **Anlage 2** – Beschreibung der Datenverarbeitungstätigkeiten konkretisiert.

1.2 Dauer des Auftrags

Die Laufzeit und Kündigung dieser Vereinbarung richtet sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrags. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses Vertrags. Das Recht zur Kündigung aus wichtigem Grund bleibt unberührt.

2. Anwendungsbereich und Verantwortlichkeit

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Der Auftraggeber ist im Rahmen dieses Vertrags für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich.

3. Rechte und Pflichten der htp

3.1 htp verwendet die Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Kunden. htp verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, die ihr überlassenen Daten an Dritte weiterzugeben. Kopien oder Duplikate werden ohne Wissen des Kunden nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind.

3.2 htp wird einen betrieblichen Datenschutzbeauftragten bestellen. Dessen jeweils aktuelle Kontaktdaten sind im Internet auf der Homepage der htp unter www.htp.net veröffentlicht.

3.3 htp setzt bei der Verarbeitung der personenbezogenen Daten nur Personen ein, die sich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

3.4 htp unterstützt den Kunden im vertraglich vereinbarten Rahmen unter Berücksichtigung der Art der Verarbeitung und der ihr zur Verfügung stehenden Informationen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DS-GVO genannten Rechte der betroffenen Person nachzukommen.

Soweit sich ein Betroffener zwecks Geltendmachung eines Betroffenenrechts unmittelbar an die htp wendet, leitet htp die Anfragen des Betroffenen zeitnah an den Kunden weiter.

3.5 htp unterstützt den Kunden bei der Einhaltung der in den Art. 33 bis 36 DS-GVO genannten Pflichten unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen. Der Auftraggeber verpflichtet sich ggf. zur Übernahme der anfallenden Mehrkosten. Unterstützungsleistungen der htp, sofern sie nicht die Meldung von Verletzungen des Schutzes personenbezogener Daten betreffen, sind angemessen und gesondert zu vergüten.

4. Drittstaatentransfer

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraums statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff DS-GVO erfüllt sind.

5. Berichtigung, Löschung und Sperrung von Daten

Vorbehaltlich abweichender Vereinbarungen zwischen den Parteien wird htp mit Beendigung dieser Vereinbarung alle personenbezogenen Daten, welche htp von dem Kunden zur Verfügung gestellt wurden, oder welche im Zusammenhang mit der Erbringung der vertragsgegenständlichen Leistung erhoben wurde, löschen.

Daten, die sich auf Speichermedien im Verfügungsbereich des Kunden befinden, sind vom Kunden datenschutzgerecht zu löschen. Sollte dies dem Kunden nicht möglich sein, wird er die htp rechtzeitig schriftlich informieren. htp ist dann berechtigt, die Daten im Auftrag des Kunden zu löschen und für den Aufwand der Löschung ein Vergütung zu verlangen.

6. Weisungsrecht des Kunden

6.1 htp wird als Auftragsverarbeiter nur im Rahmen der Weisungen des Kunden tätig.

6.2 Der Kunde weist die htp an, die Daten ausschließlich im Rahmen der getroffenen Vereinbarungen zu verwenden.

6.3 Zusätzliche Weisungen des Kunden im Hinblick auf die Verwendung der Daten, die über den vertraglich festgelegten Leistungsumfang hinausgehen, werden als Antrag auf Leistungsänderung gewertet. Führen sie zu einem Mehraufwand bei der htp, sind sie entsprechend gesondert zu vergüten. Die Vertragsparteien werden sich in diesem Fall über eine angemessene Vergütung gesondert verständigen. Bei Weisungen, deren Umsetzung für die htp nicht oder nur mit unverhältnismäßig hohem Mehraufwand möglich ist, kann die htp den Vertrag kündigen. Zusätzliche Weisungen bedürfen der Text- oder Schriftform.

6.4 htp informiert den Kunden unverzüglich, wenn sie der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. htp ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Kunden bestätigt oder geändert wird.

7. Technische und organisatorische Maßnahmen

7.1 Der Kunde und die htp werden technische und organisatorische Maßnahmen treffen, um zu gewährleisten, dass die Verarbeitung im jeweiligen Verantwortungsbereich im Einklang mit den datenschutzrechtlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet ist.

7.2 Die derzeit von htp getroffenen Maßnahmen sind in der **Anlage 3** beschrieben. Der Kunde hat die technischen und organisatorischen Maßnahmen vor dem Hintergrund der konkreten Datenverarbeitung bewertet und als angemessen akzeptiert.

7.3 Dem Kunden obliegt es, die Sicherheit der Verarbeitung und Angemessenheit des Schutzniveaus regelmäßig zu prüfen. Sollten die von htp ergriffenen Maßnahmen dem Kunden nicht oder nicht mehr genügen, wird er dies der htp unverzüglich mitteilen. Zusätzliche Maßnahmen, die über die vertraglich vereinbarten Maßnahmen hinausgehen, sind bei Mehraufwand für die htp gesondert zu vergüten. Die Parteien werden sich in diesem Fall über eine angemessene Vergütung gesondert verständigen. htp kann den Vertrag kündigen, wenn die Umsetzung von Maßnahmen für die htp nicht oder nur mit unverhältnismäßig hohem Mehraufwand verbunden ist.

7.4 Die htp kontrolliert ihrerseits die internen Prozesse und Maßnahmen, um zu gewährleisten, dass diese mit den Anforderungen der DS-GVO in Einklang stehen. Eine Änderung der getroffenen Maßnahmen bleibt der htp vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

7.5 htp wird die Einhaltung der vereinbarten Maßnahmen in geeigneter Form nachweisen. Der Nachweis kann durch die Einhaltung genehmigter Verhaltensregeln, die Zertifizierung nach einem genehmigten Zertifizierungsverfahren, aktuelle Testate, Bericht oder Berichtsauszüge, eine geeignete Zertifizierung durch Informationssicherheits- oder Datenschutzaudit oder Eigenerklärung des Auftragnehmers erfolgen.

8. Unterauftragsverarbeiter

8.1 htp darf zur Erfüllung des Auftrags Unterauftragsverarbeiter einsetzen.

8.2 Bei einer Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragsverarbeitern wird htp die Zustimmung des Kunden einholen. Die Zustimmung darf nur aus wichtigem, der htp nachzuweisenden Grund verweigert werden.
Wenn der Kunde nicht innerhalb von 2 Wochen schriftlich unter Angabe eines wichtigen Grundes widerspricht, gilt die Zustimmung des Kunden als erteilt, sofern htp auf die Folge des widerspruchslosen Verstreichens der Frist hingewiesen hat.
Wenn der Kunde gegenüber htp widerspricht, so ist htp berechtigt, den Vertrag mit einer Frist von 10 Tagen zu kündigen.

8.3 htp hat die Unterauftragsverarbeiter nach Maßgabe der gesetzlichen Vorschriften vertraglich zu verpflichten. Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/ des EWR, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

9. Kontrollrechte des Kunden

9.1 Der Kunde ist nach Maßgabe der Regelung in dieser Ziffer 9 berechtigt, die Einhaltung der in dieser Vereinbarung festgelegten Pflichten zum Schutz der personenbezogenen Daten durch htp oder Unterauftragsverarbeiter in jährlichen Abständen und anlassbezogenen zu überprüfen, wobei diese Prüfungen auf die Informationen und Datenverarbeitungssysteme beschränkt sind, die für die Erbringung der vertragsgegenständlichen Leistungen von Bedeutung sind.

9.2 Soweit htp für die vertragsgegenständlichen Leistungen Zertifizierungen durchführen und regelmäßige Prüfberichte erstellt, sind zur Ausübung der Kontrollrechte nach dieser Vereinbarung zunächst diese Zertifizierungen und Prüfberichte bzw. Auszüge daraus zu verwenden.

9.3 Nur wenn die Nachweise, Zertifikate und Prüfberichte für den Kunden nicht ausreichen, um die gesetzlichen Anforderungen an Audits und Kontrollen einzuhalten, hat der Kunde das Recht, auf eigene Kosten zusätzliche Informationen und Unterlagen anzufordern, sowie nach vorheriger Mitteilung mit einer angemessenen Frist (in der Regel mindestens 2 Wochen) eine weitergehende Prüfung der für die verarbeiteten personenbezogenen Daten relevanten Kontrollumgebung und der Sicherheitspraktiken im Rahmen der üblichen Geschäftszeiten vorzunehmen, wobei die htp-Betriebsabläufe hierdurch nicht gestört werden dürfen. Die Prüfung hat unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen der htp zu erfolgen.

9.4 htp kann für die Ermöglichung von Kontrollen durch den Auftraggeber einen angemessenen Vergütungsanspruch geltend machen.

9.5 htp ist berechtigt, nach eigenem Ermessen unter Berücksichtigung der gesetzlichen Verpflichtungen des Kunden, Informationen nicht zu offenbaren, die sensibel im Hinblick auf die Geschäfte der htp sind oder wenn htp durch deren Offenbarung gegen gesetzlich oder andere vertragliche Regelungen verstoßen würde.

9.6 Beauftragt der Kunde einen Dritten mit der Durchführung der Kontrolle, hat der Kunde den Dritten schriftlich entsprechend der Regelung in dieser Ziffer 9 zu verpflichten. Zudem hat der Kunde den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen der htp hat er dieser die Verpflichtungsvereinbarungen vorzulegen. Der Kunde darf keinen Konkurrenten der htp mit der Kontrolle beauftragen.

10. Mitteilung bei Verstößen der htp

Wenn htp Kenntnis von einer Verletzung des Schutzes personenbezogener Daten erlangt, wird htp den Kunden hiervon unverzüglich benachrichtigen.

11. Haftung

Die Haftung der htp richtet sich nach den Vereinbarungen des Hauptvertrags. Die Regelung in Art. 82 DS-GVO bleibt unberührt.

12. Sonstiges

12.1 Sämtliche Änderungen dieses Vertrags sowie Nebenabreden bedürfen der Schriftform (einschließlich der elektronischen Form). Dies gilt auch für das Abbedingen dieser Klausel selbst.

12.2 Im Fall von Widersprüchen von Regelungen dieser Vereinbarung und Regelungen aus sonstigen Vereinbarungen geht diese Vereinbarung zur Auftragsverarbeitung vor.

Anlage 2 – Beschreibung der Datenverarbeitungstätigkeiten für htp Net Business Hosting

1. Leistungen, für die personenbezogene Daten im Auftrag verarbeitet werden sollen

Webhosting, ggf. Webalizer

- htp greift zu Prüf-, Wartungs- und Installationszwecken auf die Systeme und den Storage zu.
- htp hat Zugriff auf die Kundenhomepage und leistet bei Kundenproblemen Hilfe
- Je nach Auftrag, stellt htp dem Kunden die Web Analyse Software Webalizer zur Nutzung zur Verfügung

Der konkrete Umfang, Art und Zweck der Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch htp ergeben sich aus dem Auftrag bzw. Hauptvertrag und den ggf. mitgeltenden Unterlagen (AGB, Besondere Bedingungen, Leistungsbeschreibungen).

2. Art der Daten

Folgende Arten von Daten werden erhoben, verarbeitet oder genutzt:

- Personenbezogene oder personenbeziehbare Protokolldaten (Benutzername, IP-Adresse)
- Daten, die der Verantwortliche in seinem Ermessen abspeichert
- Freiwillige Angaben der Betroffenen
- Kundennummer
- Berufs-, Branchen- oder Geschäftsbezeichnung
- Kontaktdaten
- Name
- Titel
- Akademischer Grad
- Anschrift
- Geburtsjahr
- Name, Vorname und E-Mail-Adressen
- Rufnummern
- Verkehrsdaten

Besondere Kategorien von personenbezogenen Daten:

- Keine

3. Kreis der Betroffenen

Zum Kreis der Betroffenen zählen folgende Personen/Personengruppen:

- Kunden
- Interessenten
- Abonnenten
- Beschäftigte
- Lieferanten
- Handelsvertreter
- Ansprechpartner
- Jede Kategorie von Personen, die der Kunde im Rahmen seines Geschäftszwecks erfassen möchte

Anlage 3 – Technische und organisatorische Maßnahmen

In diesem Dokument werden die technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten beschrieben, die der Auftragnehmer im Zusammenhang mit der von ihm durchgeführten Verarbeitung trifft:

I. Vertraulichkeit

1. Zutrittskontrolle

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Maßnahmen:

Schutz der Gebäude, Serverräume und Geschäftsräume durch technische Zutrittskontrollmaßnahmen (elektronische Schließanlage, Einbruchmeldeanlage); zusätzliche Maßnahmen wie spezielle Zutrittsprofile, Biometrie, Vereinzelungsschleusen, Videoüberwachung und Wachpersonal in Abhängigkeit von der Sicherheitseinstufung; Zutrittsberechtigungskonzepte

2. Zugangskontrolle

Es ist zu verhindern, dass Unbefugte die Datenverarbeitungsanlagen und –verfahren benutzen.

Maßnahmen:

Benutzerauthentifizierung, Passwortrichtlinie, Zwei-Faktor-Authentifizierung, Mehrstufige Schutzmechanismen der verwendeten IT-Systeme gegen Angriffe sowie gegen zufällige oder mutwillige Zerstörung oder Änderung u.a. durch Intrusion-Detection-Systeme, Firewalls und Malware-Filter.

3. Zugriffskontrolle

Es ist zu gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können.

Maßnahmen:
Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen

4. Trennungskontrolle

Es ist zu gewährleisten, dass die zu unterschiedlichen Zwecken erhobenen Daten getrennt verarbeitet werden.

Maßnahmen:
Mandantenfähigkeit, Trennung der verarbeitenden Systeme (z.B. durch logische Netzsegmentierung),

II. Integrität:

1. Weitergabekontrolle

Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Ferner muss überprüfbar und feststellbar sein, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Maßnahmen:
Fernwartungsverbindungen werden mittels verschlüsseltem Virtual Private Network (VPN) geschützt. , Protokollierung der Verbindungen, Transportsicherung (SSL, TLS), elektronische Signaturen

2. Eingabekontrolle

Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind.

Maßnahmen

Der Auftragnehmer erlaubt nur authentifizierten Benutzern auf der Grundlage eines rollenbezogenen Berechtigungskonzepts den Zugriff auf personenbezogene Daten. Zugriffe werden protokolliert.

III. Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle und rasche Wiederherstellbarkeit

Es ist zu gewährleisten, dass die für die Verarbeitung verwendeten Systeme gegen Ausfälle abgesichert und personenbezogene Daten somit jederzeit uneingeschränkt verfügbar und gegen Verlust geschützt sind.

Maßnahmen:

Unterbrechungsfreie Stromversorgung (USV), Umschaltung auf leistungsstarke Netzersatzanlage (Dieselaggregat), Brandmeldeanlage, direkte Aufschaltung bei der örtlichen Feuerwehr, Brandschutztüren, Löschanlagen, regelmäßige Wartungen, Notfallpläne, Redundante Systeme, virtuelle Serverumgebungen, Backup/Recovery-Konzept, Kapazitätsmanagement, Monitoring.

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Datenschutzmanagement
Incident-Management
Auftragskontrolle durch eindeutige Vertragsgestaltung, sorgfältiger Auswahl von Dienstleistern, Kontrollen