Vereinbarung

über eine

Auftragsverarbeitung nach Art 28 DSGVO

Der Verantwortliche:	Der Auftragsverarbeiter:
Delta individual Laufenstr. 20A 4222 Zwingen mit Kundennummer 40359	**hosttech GmbH** Seestrasse 15a 8805 Richterswil
(im Folgenden Auftraggeber)	(im Folgenden Auftragnehmer)

1. GEGENSTAND DER VEREINBARUNG

(1) Gegenstand dieses Auftrages sind Internetdienstleistungen im Rahmen der vom Auftragnehmer auf seinen Internetseiten angebotenen und in den jeweiligen Leistungsbeschreibungen konkretisierten Produkten. Diese Vereinbarung ist als Ergänzung zu den AGB von hosttech GmbH zu verstehen.
(2) Folgende Datenkategorien werden verarbeitet: Kontaktdaten, Vertragsdaten, Verrechnungsdaten, Bestelldaten.
(3) Folgende Kategorien betroffener Personen werden unterliegen der Verarbeitung: Kunden, Interessenten, Lieferanten, Mitarbeiter, Bewerber, Ansprechpartner & Geschäftspartner

2. DAUER DER VEREINBARUNG

Die Vereinbarung ist auf unbestimmte Zeit geschlossen und kann von beiden Parteien gemäss den definierten Kündigungsfristen des betreffenden Produktes zum Ende der Vertragslaufzeit gekündigt werden. Die Möglichkeit zur ausserordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

3. RECHTE & PFLICHTEN DES AUFTRAGGEBERS

(1) Für die Beurteilung der Zulässigkeit der Datenerhebung / - verarbeitung / -nutzung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich.
(2) Der Auftraggeber erteilt alle Aufträge oder Teilaufträge schriftlich. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und schriftlich festzulegen.
(3) Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor.
(4) Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen. Die schriftliche Bestätigung der mündlichen Weisungen sollte von Auftraggeber und Auftragnehmer zusammen mit der Vereinbarung so aufbewahrt werden, dass alle massgeblichen Regelungen jederzeit verfügbar sind.

    Weisungen können durch den Auftraggeber via myhosttech Kundencenter oder mittels Supportcode oder unterschriebenem Brief abgegeben werden.

    Sämtliche Mitarbeitenden von hosttech sind befugt, Weisungen des Auftraggebers anzunehmen und auszuführen.

    Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners ist dem Vertragspartner unverzüglich schriftlich der Nachfolger bzw. der Vertreter mitzuteilen. Falls Weisungen die unter § 1 dieses Vertrages getroffenen Festlegungen ändern, aufheben oder ergänzen, sind sie nur zulässig, wenn eine entsprechende neue Festlegung erfolgt.
(5) 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.
(6) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmässigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
(7) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmassnahmen des Auftragnehmers vertraulich zu behandeln.

4. PFLICHTEN DES AUFTRAGNEHMERS

(1) Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschliesslich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. 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.
(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 /1 zu entnehmen).

(4) Der Auftragnehmer ergreift die technischen und organisatorischen 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 wirkt an der Erstellung des Verarbeitungsverzeichnisses mit. Er stellt dem Auftraggeber die erforderlichen Angaben zur Verfügung.

(6) Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, im Auftrag des Auftragnehmers zu vernichten. 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.

(7) 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.

5. ORT DER DURCHFÜHRUNG DER DATENVERARBEITUNG

Die Datenverarbeitungstätigkeiten erfolgen in der Schweiz oder innerhalb der EU bzw. des EWR. Für die Schweiz gilt ein mit dem EU-Recht vergleichbares Datenschutzniveau. Eine Datenübermittlung in die Schweiz ist datenschutzrechtlich zulässig.

6. SUB-AUFTRAGSVERARBEITER

Der Auftragnehmer kann Sub-Auftragsverarbeiter für Serverüberprüfungen / Drittsoftwarespezifische Arbeiten hinzuziehen.
Er hat den Auftraggeber von der beabsichtigten Heranziehung eines neuen Sub-Auftragsverarbeiters so rechtzeitig zu verständigen, dass er dies allenfalls untersagen kann.
Der Auftragnehmer schliesst die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab.

Zwingen, am 13.09.2019

Der Auftraggeber:

Mireille Vargas, Delta individual

Richterswil, am 13.09.2019

Der Auftragnehmer:

hosttech GmbH
Patrizia Burger
Datenschutzmanagerin

ANLAGE ./1 – TECHNISCH-ORGANISATORISCHE MASSNAHMEN

VERTRAULICHKEIT

Zutrittskontrolle:

- Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen:
- dokumentierte Schlüssel- oder -Chipkartenvergabe
- elektrische Türöffner mit Zutrittsstatistik
- Alarmanlagen
- Videoüberwachung

Zugangskontrolle:

- Bei Hauptauftrag Webhosting & Managed Server (auf Systemebende)
  - Schutz vor unbefugter Systembenutzung
  - Kennwortschutz (einschliesslich entsprechender Policy)
  - Zugriff nur für Mitarbeiter von Auftragnehmer
  - automatische Sperrmechanismen sofern möglich
- Bei Hauptauftrag Dedicated Server & Cloudserver
  - Server-Passwörter können nach erstmaliger Inbetriebnahme nur vom Auftraggeber selbst geändert werden
  - Server-Passwörter sind dem Auftragnehmer nicht bekannt
  - Kennwortschutz (einschliesslich entsprechender Policy)

Zugriffskontrolle:

Zur Verhinderung von unbefugtem Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems.

- Bei internen Systemen des Auftragnehmers
  - Schutz vor unberechtigten Zugriffen durch regelmässige Sicherheitsupdates und Backups
  - Standardprozess für Berechtigungsvergabe
  - Protokollierung von Zugriffen
  - periodische Überprüfung der vergebenen Berechtigungen
- Bei Hauptauftrag Webhosting & Managed Server (auf Systemebene)
  - Schutz vor unberechtigten Zugriffen durch regelmässige Sicherheitsupdates und Backups
  - Standardprozess für Berechtigungsvergabe
  - Protokollierung von Zugriffen
  - periodische Überprüfung der vergebenen Berechtigungen
- Bei Hauptauftrag Dedicated Server & Cloudserver
  - Die Verantwortung der Zugriffskontrolle liegt beim Auftraggeber

Klassifikationsschema für Daten:

Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

INTEGRITÄT

Weitergabekontrolle:
Zur Verhinderung von unbefugtem Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport.

- Mitarbeiter werden regelmässig im Datenschutzrecht geschult
- Mitarbeiter sind auf das Datengeheimnis verpflichtet

Eingabekontrolle:

- Bei internen Systemen des Auftragnehmers
  - Eingabe der Daten durch den Auftraggeber oder berechtigte Mitarbeiter des Auftragnehmers
  - Protokollierung von Änderungen
- Bei Hauptauftrag Webhosting & Managed Server
  - Eingabe der Daten durch den Auftraggeber oder berechtigte Mitarbeiter des Auftragnehmers
  - Protokollierung von Änderungen
- Bei Hauptauftrag Dedicated Server & Cloudserver
  - Die Verantwortung der Eingabekontrolle liegt beim Auftraggeber
  - Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (sofern möglich)

VERFÜGBARKEIT UND BELASTBARKEIT

- Rasche **Wiederherstellbarkeit** (sofern Backups verfügbar & im betroffenen Produkt enthalten)
- **Löschungsfristen:** Sowohl für Daten selbst als auch Metadaten wie Logfiles.

Verfügbarkeitskontrolle:

- Bei internen Systemen des Auftragnehmers
  - Tägliche Sicherung aller relevanten Daten
  - Festplattenspiegelung
  - Monitoring aller relevanten Systeme
  - unterbrechungsfreie Stromversorgung (USV)
  - Virenschutz, Firewall, SPAM-Filter
  - Meldewege und Notfallpläne
  - Security Checks auf Infrastruktur- und Applikationsebene
  - Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern
- Bei Hauptauftrag Webhosting & Managed Server
  - Tägliche Sicherung aller relevanten Daten (sofern im Angebot enthalten / gebucht)
  - Festplattenspiegelung
  - Monitoring aller relevanten Systeme
  - unterbrechungsfreie Stromversorgung (USV)
  - Virenschutz, Firewall, SPAM-Filter (sofern im Angebot enthalten / gebucht)
  - Meldewege und Notfallpläne
  - Security Checks auf Infrastruktur- und Applikationsebene
  - Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern

- Bei Hauptauftrag Dedicated Server & Cloudserver
  - Die Verantwortung der Datensicherung liegt beim Auftraggeber
  - unterbrechungsfreie Stromversorgung (USV)

Datensicherung:

- Bei internen Systemen des Auftragnehmers
  - Physikalische oder logische Trennung der Daten
  - Datensicherung physikalisch oder logisch getrennt von Ursprungsdaten
- Bei Hauptauftrag Webhosting & Managed Server
  - Physikalische oder logische Trennung der Daten
  - Datensicherung physikalisch oder logisch getrennt von Ursprungsdaten
- Bei Hauptauftrag Dedicated Server & Cloudserver
  - Die Verantwortung der Trennungskontrolle liegt beim Auftraggeber

VERFAHREN ZUR REGELMÄSSIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

- Datenschutz-Management, einschliesslich regelmässiger Mitarbeiter-Schulungen;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen;

Auftragskontrolle:

- Keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers
  - eindeutige Vertragsgestaltung
  - formalisiertes Auftragsmanagement
  - Regelmässige Mitarbeiterschulungen im Datenschutzrecht
  - AGB & Datenschutzerklärung enthalten detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers