Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO als Anlage zu einem oder mehreren vom Auftraggeber genutzten Vertrag oder Verträgen

Zwischen der Firma

IT-Service & Software Entwicklung
Dürrenberg 97
09477 Jöhstadt
Deutschland

– Nachfolgend „**Auftragnehmer**“ genannt –

und

Firma:
Name:
Straße, Hausnummer:
Postleitzahl, Ort:
Land:
Kundennummer:

– Nachfolgend „**Auftraggeber**“ genannt –

Präambel

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im Einzelvertrag (nachstehend „Vertrag“) in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers, oder durch den Auftragnehmer Beauftragte personenbezogene Daten (nachstehend „Daten“) des Auftraggebers verarbeiten.

Diese Anlage ist nur gültig in Verbindung mit einem aktiven Vertrag über die folgenden Produkte:

Hosting
Webhosting, E-Mail Hosting

Support
Technischer Software- und Hardware-Support

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

1) Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung. Gegenstand dieser Anlage ist nicht die originäre Nutzung oder Verarbeitung von personenbezogenen Daten durch den Auftragnehmer. Im Zuge der Leistungserbringung des Auftragnehmers als IT-Dienstleister im Bereich des Hostings, des Supports bzw. der Administration von Server-Systemen kann auf Seiten des Auftragnehmers ein Zugriff auf personenbezogene Daten allerdings nicht ausgeschlossen werden. Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Anlage nicht darüber hinausgehende Verpflichtungen ergeben.

§ 2 Anwendungsbereich und Verantwortlichkeit

1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind.

Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich („Verantwortlicher“ i.S.v. Art. 4 Nr.7 DS-GVO).

2) Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form, oder in einem elektronischen Format („Textform“) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt, oder ersetzt werden („Einzelweisung“). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

§ 3 Pflichten des Auftragnehmers

1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne von Art. 28 Abs. 3 lit. a) DS-GVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Die Durchführung von rechtswidrigen Weisungen darf der Auftragnehmer ablehnen.
2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutzgrundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen.
3) Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen.

4) Die Beschreibung Technischer und Organisatorischer Maßnahmen gemäß Anhang 1 ist Bestandteil dieser Vereinbarung.
   Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.
   Der Auftragnehmer unterstützt soweit erforderlich den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gemäß Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 und 34 DS-GVO genannten Pflichten.
5) Der Auftragnehmer stellt sicher, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner stellt der Auftragnehmer sicher, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben, oder einer angemessenen gesetzlichen Schweigepflicht unterliegen. Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrags fort.
6) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.
7) Für alle im Rahmen dieser Anlage anfallenden Datenschutzfragen sind die Kontaktdaten:
   Adresse: Die auf Seite 1 genannte Adresse des Auftragnehmers
   E-Mail: datenschutz@its-se.de
   Tel: +49 (0)37343 219 751
8) Der Auftragnehmer stellt sicher, seinen Pflichten nach Art. 32 Abs.1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.
9) Der Auftraggeber hat selbst jederzeit umfassenden Zugriff auf die Daten, so dass es einer Mitwirkung des Auftragnehmers insbesondere auch zu Berichtigung, Sperrung, Löschung etc. nicht bedarf. Soweit eine Mitwirkung des Auftragnehmers erforderlich ist, ist der Auftragnehmer hierzu gegen Erstattung der anfallenden Kosten verpflichtet.

Dem Auftraggeber steht in diesem Fall ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung gemäß Art. 29 i.V.m. 28 DSGVO zu. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

10) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.
11) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

§ 4 Pflichten des Auftraggebers

1) Der Auftraggeber hat den Auftragnehmer unverzüglich zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt § 3 Abs. 11 dieser Anlage entsprechend.

§ 5 Anfragen betroffener Personen

1) Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen an den Auftraggeber weiterleiten, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Ist der Auftraggeber auf Grund geltender Datenschutzgesetze verpflichtet, Auskünfte zur Erhebung, Verarbeitung und / oder Nutzung von Daten zu erteilen, wird der Auftragnehmer den Auftraggeber dabei, im Rahmen seiner Möglichkeiten und soweit vereinbart, bei der Bereitstellung dieser Informationen unterstützen.

Eine diesbezügliche Anfrage hat der Auftraggeber schriftlich an den Auftragnehmer zu richten und diesem die hierdurch entstandenen Kosten zu erstatten. Der Auftragnehmer haftet bei Erfüllung seiner Pflichten nicht dafür, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig, oder nicht fristgerecht beantwortet wird.

§ 6 Nachweismöglichkeiten

1) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten, ohne Störung des Betriebsablaufs nach Anmeldung und unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung verlangen. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.
2) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 1 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

7 § Drittstaatentransfer

1) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet überwiegend in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Ausnahmen sind der Liste gem. §8 Abs. 2 dieser Anlage zu entnehmen.

§ 8 Subunternehmer (weitere Auftragsverarbeiter)

1) Mit der Hinzuziehung von verbundenen und fremden Unternehmen zur Wartung, Pflege der Rechenzentrumsstruktur, Telekommunikationsdienstleistungen und Benutzerservice durch den Auftragnehmer ist der Auftraggeber einverstanden.
2) Eine Liste der aktuell eingesetzten Unterauftragnehmer steht dem Auftraggeber in Anlage 2 zur Verfügung.
   Eine weitere Auslagerung oder der Ersetzung aufgeführter Subunternehmer durch den Unterauftragnehmer oder Auftragnehmers bedarf der ausdrücklichen Zustimmung des Auftraggebers.
3) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen. Die volle Verantwortung für die vom Auftragnehmer eingeschalteten Subunternehmer bleibt beim Auftragnehmer.

Für den Auftraggeber	Für den Auftragnehmer
_____	Jöhstadt,
Ort, Datum	Ort, Datum
_____	_____
Unterschrift	Unterschrift

Anlage 1 - Technische und organisatorische Maßnahmen

- **Zutrittskontrolle** - Maßnahmen um zu verhindern, dass Unbefugte Zutritt (räumlich zu verstehen) zu Datenverarbeitungsanlagen erhalten, mit welchen personenbezogene Daten verarbeitet werden.
  1) Manuelles Schließsystem
  2) Personal überwacht den Zutritt
  3) Sorgfältige Auswahl von Reinigungspersonal
  4) Aufenthalt von Besuchern nur in Anwesenheit von Mitarbeitern

- **Zugangskontrolle** - Maßnahmen um zu verhindern, dass Datenverarbeitungsanlagen von Unbefugten benutzt werden können.
  1) Zuordnung von Benutzerrechten
  2) Authentifikation mit Benutzername / Passwort
  3) Protokollierung von Zugriffen
  4) Einsatz von Intrusion Prevention System
  5) Der Auftragnehmer vermietet die Nutzung der Datenverarbeitungsanlage gemäß dem jeweiligen Produkt an den Auftraggeber. Der Auftraggeber entscheidet welche personenbezogenen Daten in welcher Weise verarbeitet werden. Der Auftragnehmer hat keinerlei Einfluss auf die durch den Auftraggeber durchgeführten Datenverarbeitungsvorgänge im Sinne des §46 Abs. 2 BDSG.
  6) Der Auftraggeber ist für die regelmässige Änderung der Zugangspasswörter verantwortlich.
  7) Der Auftragnehmer sorgt für die technische Einsatzbereitschaft des Systems entsprechend den vertraglichen Vereinbarungen.
- **Zugriffskontrolle** - Gewährleisten, dass nur Berechtigte auf Daten zugreifen können und diese nicht unbefugt gelesen, verändert, kopiert oder entfernt werden können.
  1) Authentifikation mit Benutzername / Passwort
  2) Protokollierung von Zugriffen
  3) Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte
  4) Verwaltung der Rechte durch Systemadministrator
  5) Anzahl der Systemadministratoren auf das „Notwendigste“ reduziert
  6) Bereits unter Zugangskontrolle Punkt 5 und Punkt 6 ausgeführt

7) Alle Mitarbeiter des Auftragnehmers sind gemäß BDSG zur Einhaltung der datenschutzrechtlichen Gesetze und Regelungen verpflichtet und entsprechend geschult.

- **Weitergabekontrolle** - Gewährleisten, dass Daten bei der elektronischen Übertragung/Transport nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.
  1) Dokumentation der Datenempfänger, der übermittelten Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
  2) Verschlüsselung von Funknetzen (WLAN)
  3) Dem Auftraggeber obliegt es durch eine Verschlüsselung, z.B. SSL dafür zu sorgen, dass die übertragenen Daten nicht lesbar sind.
  4) Alle Administrations-Werkzeuge können über eine verschlüsselte Verbindung bedient werden.

- **Eingabekontrolle** - Gewährleisten, dass nachträglich überprüft werden kann, ob und wer Daten verändert oder entfernt hat.
  1) Bereits unter Zugangskontrolle Punkt 5 ausgeführt
  2) Protokollierung von Zugriffen

- **Auftragskontrolle** - Gewährleisten, dass Daten, die im Auftrag verarbeitet werden, nur entsprechend den Anweisungen des Auftraggebers verarbeitet werden können.
  1) Bereits unter Zugangskontrolle Punkt 5 ausgeführt
  2) Verpflichtung der Mitarbeiter auf das Datengeheimnis gemäß §53 BDSG
  3) Kontrollrechte durch den Auftraggeber
  4) Der Auftragsverarbeiter haftet dem Verantwortlichen gegenüber uneingeschränkt für Datenschutzverstöße des Subunternehmers.

- **Verfügbarkeitskontrolle** - Gewährleisten, dass Daten gegen zufällige Zerstörung oder Verlust geschützt sind.
  1) Unterbrechungsfreie Stromversorgung (USV) und Notstromaggregat
  2) USV filtert zusätzlich vollständig alle Unregelmäßigkeiten oder Störungen des Stromversorgungsnetzes.

3) Schutz-Steckdosenleisten (zentral in Grundversorgung)
4) Tägliche Datensicherungen auf vom Server getrenntem Speicherplatz, welche regelmässig gelöscht werden.
5) Jeder Kunde hat zudem die Möglichkeit zusätzliche Sicherungen seiner Daten über seinen Control-Panel Zugang zu erstellen und bei Bedarf wiederherzustellen.

- **Trennungsgebot** - Gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden

1) Die Bereiche in welchen die Kundendaten gespeichert werden, sind logisch voneinander getrennt.
2) Durch die Anwendung eines Berechtigungskonzeptes, kann jeder Kunde nur auf seine Daten zugreifen.
3) Bereits unter Zugangskontrolle Punkt 5 ausgeführt

Anlage 2 - Unterauftragnehmer

Firma	Anschrift	Leistung
HEXONET GmbH	HEXONET GmbH Talstraße 27 66424 Homburg	Domain-Registrierung